# Executive Summary

The Aerospace Industry Association (AIA) appreciates the opportunity to provide the Department of Defense with our perspectives on the important topics below.  Our member companies encompass the breadth of the Defense Industrial Base (DIB) and are committed to ensuring the mission of the DoD.  AIA members believe strongly in the power of Artificial Intelligence (AI) to deliver advantage to the U.S. warfighter.  Enabling processes, tools, expectations, regulations, programs, and standards are crucial to successful deployment of AI within the DoD capability set.

AIA members recommend that the DoD consider a unified approach to data availability. Establishing clear expectations on how data is provided, accessed, shared, assessed, related, and owned will be crucial to the deployment of AI systems.

Additionally, questions on Intellectual Property (IP) must be addressed.  The DIB advocates for recognition of the need for investment to train models and the associated IP protections that will incentivize such investment.

The rapid advances in AI capabilities have the potential to disrupt the DoD and DIB workforce.  AIA recommends the DoD establish programs to assess the impact of AI on jobs and to provide training that will enable employees at all levels of the DIB to safely and effectively use AI.

AI offers the promise of identifying supply chain constraints and concerns if the right data is integrated into models.   Such models offer the opportunity for enhanced supply chain management, resilience, and security through supply chain discovery, monitoring, and modeling.

Addressing cybersecurity implications will be needed, and include the establishment of requirements around data governance, testing, transmission, and ownership, as well as the security expectations for the models in use.

In summary, AIA membership believes that establishing clear guidance, policies, and standards; investing in data and AI infrastructure; fostering collaboration and information-sharing; streamlining acquisition and procurement processes; incentivizing innovation and R&D; and creating intellectual property protections will enable deployment of AI within the DoD and the DIB.

# Infrastructure/Supply Chain Resilience

***1. 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?***

AI progress will depend on large amounts of data and open conversations on data rights for national security purposes. The government has many such datasets, and the U.S. government should define processes to make these datasets accessible for model training while addressing the security of such data. The DoD should also invest in interoperable, federated infrastructure, advance the data, analytics, and AI ecosystem, and improve foundational data management.

The DoD Chief Data and AI Office (CDAO) recently communicated at the Advantage DoD 2024 AI symposium in March that CDAO will be opening access to government data over the next year. This initiative includes publishing APIs to government data and a federated data catalog, creating a hub for labeled data, and offering experimentation opportunities for industry to receive direct feedback on their products. To maximize the benefits of this initiative, the DoD should consider investments that accelerate secure access to these datasets for DIB members. To accelerate and maximize adoption of AI, the DIB needs fair, equitable, and secure/trusted access to datasets. The DoD should carefully consider which data to provide, emphasizing the availability, compatibility, and quality of datasets. Additionally, the DoD needs to establish policy for ownership for shared datasets that may grow or change over time.

Regulations must be established to determine the ownership of resulting AI models, recognizing the value of both government-supplied data and private entity investments. These regulations could follow the existing model of intellectual property ownership residing with the industry, while structuring license and usage rights to acknowledge the contributions of both parties. Proprietary information must be protected. When evaluating AI system outputs as deliverables, it is essential to establish clear standards that the U.S. government will accept under a contract. Additionally, restricted access and classification of source data and resulting trained models may limit the potential of AI.

AI can provide capabilities to aggregate disparate datasets where the constituent datasets are not classified, but the aggregate information would be classified. Consideration for such establishment or elevation of classification should be included in considering whether to release data sets to the public.

For hybridized datasets that combine U.S. government data with other sources, it is crucial to develop a framework that clearly defines ownership and usage rights. This framework should ensure that both the government, allies, and private entities benefit from the hybridized datasets while maintaining data integrity and security.

The DoD should assess the opportunity and need to build its own foundational and frontier models, making these available to the DIB for incorporation into AI systems. While this may require significant investment, relying solely on commercial and open-source models introduces risks and dependencies for the DoD. Furthermore, the DoD should consider investing in developing a framework for the Independent Verification and Validation (IV&V) of AI in defense systems. This includes developing standardized approaches to evaluating AI risk, creating playbooks of controls, Concepts of Operations (CONOPS), architectural frameworks, and design patterns to mitigate these risks. The risks associated with AI in a system depend on how AI impacts overall system behavior. By thoroughly understanding these impacts, risk levels can be managed through CONOPS or system architecture and design decisions. Approaches such as Systems-Theoretic Process Analysis (STPA) can help identify potential hazards, understand system interactions, and establish controls to prevent unsafe and undesired behaviors.

Foundational investments have already been made, including standards on autonomy such as Department of Defense Directive 3000.09, “Autonomy in Weapons Systems,” and the establishment of Chief Digital and AI Officers within government agencies. Additionally, the DoD CDAO’s Responsible AI (RAI) Toolkit provides a centralized process to help identify, track, and improve the alignment of AI projects with AI Ethical Principles. The Toolkit offers modular assessments, tools, and artifacts that span the entire AI product lifecycle, ensuring responsible AI application development based on established frameworks like the NIST AI Risk Management Framework and the IEEE 7000 Standard.

The DoD should consider using public-private mechanisms such as the A&D CDAO roundtable to share leading practices and approaches for responsible AI. Aligning internal CDAO efforts on data governance, data standards, and other areas with agency efforts to build AI competency within the DIB is also crucial.

The DoD should invest in AI-enabled design and manufacturing techniques to enable the efficient and scalable production of defense systems. Foundational investments are being made by solution providers for the design and manufacturing of defense systems, including new technologies like copilots, computer vision, and natural language processing to enhance productivity, catch errors, and improve quality. Advanced manufacturing technologies and capabilities, such as additive manufacturing (3D printing), robotics, and automation, can support the production of AI-enabled defense systems by improving efficiency and flexibility in manufacturing processes.  AI systems can enable the DoD to identify critical components and technologies, diversify suppliers, and establish redundancy to mitigate risks of supply chain disruption or compromise.

Continued work towards establishing standards and certification processes for AI systems, including defining technical specifications, performance requirements, and safety standards, will facilitate interoperability, reuse, and reliability across different AI systems. The development and promotion of best practices and guidelines for the design, development, and deployment of responsible AI systems in defense will drive accountability for ethical AI, data privacy, cybersecurity, and human-machine teaming. Investing in testing and evaluation infrastructure to assess the performance, reliability, and safety of AI systems by establishing test ranges, simulation environments, and evaluation criteria to validate the effectiveness and suitability of AI technologies can leverage similar concepts and previous efforts in the extended reality (XR), modeling and simulation, and digital twin collaborative domains. Examples include the RAPID Lab for XR, the Central Florida Tech Grove for modeling and simulation, and the Knights Digital Twin Initiative for digital twins.

The application of artificial intelligence to software supply chains (SSCs) within the defense industrial base (DIB) holds significant promise for improving cybersecurity posture, ensuring stricter compliance with National Institute of Standards and Technology (NIST) controls, and increasing user confidence in software that incorporates modules and libraries from external repositories. To secure SSCs, it is crucial to implement preventive strategies against attacks. This can be achieved by establishing a security baseline and engaging in robust and continuous behavioral monitoring practices. The most sophisticated of these behavior-based methods involves utilizing AI models to forecast, infer, predict, correlate, and pinpoint likely weaknesses, potential attack vectors, and avenues of approach within SSC-embedded software. AI-powered systems can continuously monitor SSCs in real time, identifying suspicious activities and flagging actions that could otherwise allow unauthorized access.

Most of the technical guidance for securing SSCs across the firms and organizations that make up the DIB is generated by NIST. A longstanding federal entity originally involved in the standardization of weights, measures, and metrology measurements, NIST released its landmark cybersecurity framework (CSF) as Version 1.0 in 2014. The framework quickly found widespread adoption among commercial firms and government IT departments and has been updated and expanded several times since. At its core, the CSF details a set of best-practice cybersecurity activities, standardized tools, and references, and further describes the "desired outcomes" of applying the framework across an organization. NIST CSF 2.0, completed in February 2024, now explicitly aims to help all organizations — not just those in critical infrastructure, its original target audience — manage and reduce risks. NIST has updated the CSF's core guidance and created a suite of resources to help all organizations achieve their cybersecurity goals, with added emphasis on governance and supply chains.

While NIST is not a traditional regulatory agency, the use of the CSF has become mandatory for federal agencies. Other NIST guidance, including the “Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities” (NIST Special Publication [SP] 800-218) and the “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations” (NIST SP 800-161r1), provides additional discussion of vulnerabilities and SSC security controls at both a technical and conceptual level. In collaboration with the private and public sectors, NIST has developed a framework to better manage risks to individuals, organizations, and society associated with AI. The NIST AI Risk Management Framework (AI RMF) is intended for voluntary use and aims to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. Released on January 26, 2023, the Framework was developed through a consensus-driven, open, transparent, and collaborative process that included a Request for Information, several draft versions for public comments, multiple workshops, and other opportunities to provide input. It is intended to build on, align with, and support AI risk management efforts by others.

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

Smaller organizations within the DoD supply chain often face significant challenges due to limited resources for personnel training to effectively utilize AI in their products and services. These constraints also limit their capacity to enhance off-the-shelf large language models or build custom models. Consequently, it is crucial for the DoD to actively collaborate with commercial LLM providers and provide mechanisms to ensure that these smaller entities can still benefit from advanced AI technologies.

Companies that have not historically served the defense market may lack awareness of the stringent expectations regarding reliability, safety, cybersecurity, and quality demanded by the DoD. To address this, there must be established standards and processes to assess vulnerabilities in AI incorporated into defense systems and services, and assessment of contract responses must account for compliance to these standards.

Today’s AI landscape increasingly includes open-source software, models, and datasets. Therefore, the DoD should focus on open-source security and software supply chain risk management (SSCRM). Implementing standards and requirements around an “AI Bill of Materials” (AI BoM) — a comprehensive inventory of all components involved in the creation and deployment of AI in defense systems — is essential. This concept is akin to the Software Bill of Materials (SBOM), which lists components and dependencies, especially for open-source software.

Intellectual property (IP) protection for defense contractors’ AI models within a cloud ecosystem is another critical area. Investments are needed to relieve the cost burden on small businesses, preventing them from exiting the DIB due to DoD cybersecurity requirements like the Cybersecurity Maturity Model Certification (CMMC) and the NIST Risk Management Framework. Increased supply chain visibility and transparency are required to develop AI-enabled solutions that mitigate supplier risks and cost concerns.

AI systems raise several ethical concerns, including bias, privacy, accountability, and safety impacts. The DoD must address these issues by ensuring that AI systems are developed and deployed in a manner that aligns with ethical principles and legal frameworks. Given that AI systems heavily rely on data, algorithms, and software, they are vulnerable to cyber threats. The DoD needs to secure the supply chain for AI systems with robust cybersecurity measures to protect against data breaches, hacking attempts, and other cyber-attacks.

High-quality data is essential for training and operating AI systems effectively. However, the data supply chain can be vulnerable to manipulation, tampering, or contamination. The DoD must establish mechanisms to ensure the integrity and quality of data used in AI systems, including data collection, storage, and sharing processes. Additionally, AI systems rely on hardware components and software frameworks, which can have vulnerabilities that adversaries could exploit. The DoD needs to assess and mitigate risks associated with the supply chain for AI hardware and software, ensuring the authenticity and integrity of components and software used in defense systems.

The DoD's reliance on a global supply chain for various components and technologies introduces vulnerabilities, such as potential disruptions, intellectual property theft, or compromised components. To mitigate these risks, the DoD needs to diversify its supply chain and reduce reliance on single-source suppliers. AI can assist analysts by suggesting frequencies for rescanning, supplementing threat assessments of infrastructure, automating threat intelligence processing, and expediting cybersecurity risk management. The security of SSCs in the DIB can benefit from AI as a recommendation engine for communicating the probability of compromise.

For DoD cybersecurity analysts, AI-driven automation can provide insights into how closely software capabilities deployed on military and government networks adhere to NIST compliance standards. Reflecting the most up-to-date set of vulnerabilities within a system security plan could significantly improve upon the existing practice of relying on manual internal scanning. AI can enable human-in-the-loop workflows to optimize the integration of processed threat intelligence and better identify vulnerabilities per software and/or operating system.

The DoD should focus particularly on assessing and advancing the digital maturity of the DIB, particularly at lower tiers. Given that AI and certainly Gen AI are inexorably dependent on a solid data foundation, the gaps in technology maturity, investment capacity, etc. have significant potential to limit the ability of the full DIB to take advantage of AI.

***3. 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?***

Industries that have historically focused on physical and industrial manufacturing may not have made significant investments in software, computing, and personnel necessary to apply AI to their work. However, these organizations stand to benefit significantly from the application of AI to automation processes, identifying quality improvement opportunities, optimizing maintenance schedules, increasing safety and cybersecurity, and improving environmental analysis.

The effectiveness of AI depends on a robust digital core and data foundation. Tier one and two members of the Defense Industrial Base (DIB) with more mature digital capabilities will face challenges in improving confidence, trust, and connectivity in their data. Meanwhile, lower-tier DIB members with limited digital infrastructure may struggle to scale AI solutions effectively until they achieve a higher level of digital maturity.

Incorporating AI into existing manufacturing operations can require significant investment in retooling, retraining the workforce, and integrating with existing systems. AI systems also raise ethical concerns, such as bias, privacy, accountability, and safety impacts. The DoD needs to address these issues by ensuring that AI systems are developed and deployed in a manner that aligns with ethical principles and legal frameworks. Given that AI systems heavily rely on data, algorithms, and software, they are vulnerable to cyber threats. The DoD must ensure that the supply chain for AI systems is secure, with robust cybersecurity measures in place to protect against data breaches, hacking attempts, and other cyber-attacks.

AI systems require large amounts of high-quality data to train and operate effectively. However, the data supply chain can be vulnerable to manipulation, tampering, or contamination. The DoD needs to establish mechanisms to ensure the integrity and quality of data used in AI systems, including data collection, storage, and sharing processes. Additionally, AI systems rely on hardware components and software frameworks, which can have vulnerabilities that adversaries could exploit. The DoD needs to assess and mitigate risks associated with the supply chain for AI hardware and software, ensuring the authenticity and integrity of components and software used in defense systems.

The DoD’s reliance on a global supply chain for various components and technologies introduces vulnerabilities, such as potential disruptions, intellectual property theft, or compromised components. To mitigate these risks, the DoD needs to diversify its supply chain and reduce reliance on single-source suppliers. Aerospace and defense manufacturers face challenges in integrating AI into their existing systems and processes due to the complexity and cost of retrofitting legacy systems with AI. Ensuring interoperability and compatibility among different AI systems and platforms is a significant challenge.

The software development and IT services sector faces challenges in developing AI algorithms and software frameworks that are robust, secure, and adaptable to defense applications. Ensuring the reliability and safety of AI systems is critical, especially in defense systems where lives and national security are at stake. As AI systems become more prevalent in defense systems, the cybersecurity and information assurance sectors face challenges in protecting these systems from cyber threats. Adversaries may attempt to exploit vulnerabilities in AI algorithms, data, or infrastructure to compromise defense systems. Developing robust cybersecurity measures and ensuring the integrity of AI systems is crucial.

Traditionally, access to trusted and assured datasets has been limited to integrators. To proliferate AI across all sectors and share data between different entities, this paradigm must shift to democratize datasets. This change will enable broader access and utilization of AI technologies, fostering innovation and enhancing the overall security and effectiveness of defense systems.

## Workforce

***4. 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?***

To effectively leverage the expertise of existing contractors while harnessing the capabilities of small and innovative companies, the Department of Defense (DoD) should create mentor-protégé programs. These programs could include specific Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) funding targeted at non-traditional defense contractors (such as with AFWERX and the DARPA Grand Challenge programs). For these programs to be impactful at scale, mentor companies should be allowed to have several protégés concurrently, with the number of protégés tailored to the size and scope of the mentor company. The current blanket limit of three protégés per mentor significantly reduces the potential impact of such a program.

To engage non-traditional defense contractors and small businesses, the DoD should actively promote awareness and outreach efforts. This can involve hosting industry days, conferences, or workshops to educate and inform these entities about defense needs, requirements, and opportunities in AI technology development. Such initiatives would help bridge the gap between the DoD and potential new contributors to defense innovation.

Establishing clear guidelines and policies regarding intellectual property rights is another crucial step. By providing flexible licensing agreements or intellectual property sharing arrangements, the DoD can incentivize non-traditional defense contractors and small businesses to participate in AI technology development. Clear and fair policies will encourage more entities to contribute their innovations without fear of losing their intellectual property.

Additionally, the DoD should establish and invest in university academic programs to train both current students and the established workforce. Mini or short certification programs are powerful tools to rapidly retool human capital, ensuring that the workforce remains skilled and adaptable to new technologies and methodologies.

Finally, funding a DoD-National Institute of Standards and Technology (NIST) testbed to develop new materials for advanced manufacturing related to AI, including integration with other technologies, is essential. This initiative would support the development of cutting-edge materials and processes, further enhancing the DoD's capabilities in advanced manufacturing and AI integration.

***5. 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?***

To effectively address the evolving landscape of artificial intelligence (AI) within the Department of Defense (DoD), it is essential to implement joint training initiatives that include both industry and DoD participants. Conducting surveys among DoD staff and the Defense Industrial Base (DIB) personnel will help assess the current state of AI awareness and capabilities. These insights can then inform the development of targeted plans to bridge identified gaps.

AI and related skills, such as data analysis and prompt engineering, should be considered fundamental for skill development across the civilian ecosystem, including apprenticeships, colleges, and universities. The DoD can collaborate with educational institutions to integrate these skills into broader curricula, thereby promoting AI literacy and preparing a workforce adept in these critical areas.

Fostering collaboration with the DIB on research and development (R&D) activities is another crucial step. This can be achieved through joint R&D projects, technology transfer programs, and shared access to innovation centers and test facilities. Such collaborative efforts will enhance the development of cutting-edge skills and capabilities within the workforce.

The DoD should also focus on developing and supporting training and education programs centered on AI technologies and their defense applications. Partnering with academic institutions, industry associations, and research organizations can provide specialized training, certifications, and degree programs that align with workforce needs.

Establishing workforce development initiatives that promote continuous learning and upskilling is vital. This includes providing resources for professional development, offering apprenticeships or internships, and supporting career advancement opportunities within the DIB.

The DoD should make a concerted investment in foundational training around AI for staffers, with a focus on understanding capabilities and limitations of AI-supported workflows.  Simply delivering AI tools without consideration for the processes into which the tools will be integrated is a likely path for limited return on investment and frustration for users.

Finally, the DoD must implement effective recruitment and retention strategies to attract and retain skilled professionals in AI technology. Offering competitive salaries, benefits, and incentives, along with creating a supportive and inclusive work environment that fosters innovation and collaboration, will be key to maintaining a robust and capable workforce.

## Innovation

***6. 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?***

Training a model often requires significant private investment. Defining ownership of models trained with government data is crucial to assure the defense industrial base (DIB) that they can recover their investment in model training. Regulations regarding ownership of these models could follow the existing efficient model of intellectual property (IP) ownership residing with the industry. License and usage rights should be structured to acknowledge both the value of government-supplied data and the private entity’s investment.

When open-source architectures are utilized, it is important to identify IP ownership separately for architectures and models. This distinction will support private entities in investing in model training. The Department of Defense (DoD) and the DIB should consider IP, security, and other considerations regarding the data used to train AI models. Providing appropriate legal and financial protections will support the ongoing development of AI solutions within the DoD and the DIB.

Developing AI-enabled defense systems often involves collaboration between multiple entities, including defense primes, non-traditional contractors, and research institutions. Determining ownership and sharing of IP rights in collaborative projects can be complex. Clear agreements and IP frameworks should be established to address these challenges. AI-enabled defense systems often involve complex algorithms, software, and data that may have IP rights associated with them. Determining ownership and control of these IP rights can be challenging, especially when multiple entities are involved in the development process.

The DoD can provide incentives for collaboration and information sharing among entities within the DIB. This can include funding opportunities, grants, or research and development contracts that prioritize collaborative efforts and encourage the sharing of IP. Additionally, the DoD can promote standardization and interoperability in AI-enabled defense systems. By establishing common frameworks, protocols, and interfaces, the DoD can facilitate the integration of different components and technologies without infringing on IP rights.

***7. 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?***

As noted in response to Question 6, addressing intellectual property concerns is crucial for the Defense Industrial Base (DIB) to invest in model training and deployment for defense systems and services. Ensuring clear and robust IP protections will foster confidence and encourage investment in these critical areas.

Creating collaborative environments, such as conferences, information exchanges, and workshops, is essential for identifying datasets with the highest potential value to the Department of Defense (DoD). These environments should be accompanied by detailed plans outlining the processes to make these datasets available.

All data generated by DoD systems, whether in development or deployment, should be stored, mined, and made accessible for artificial intelligence (AI) and machine learning (ML) applications. To promote greater innovation, this data should be made available to the DIB, with requirements for maintaining the history, provenance, and pedigree of datasets and models. Ensuring data and model traceability is vital. The DoD should assign data product owners for all data sources, making the data centrally discoverable and accessible via APIs.

The DoD can consider employing contractual incentives, such as favorable payment terms, preferred supplier status, or other mechanisms, all supported by clear IP protections, to encourage targeted goals like data availability. Additionally, the DoD can collaborate with the broader technology ecosystem, including cloud providers and AI companies, to publish standard mechanisms for data exchange and data architectures.

Creating a secure and centralized platform is necessary to allow various stakeholders to share information, research findings, and best practices related to AI adoption in defense systems. Continued funding for defense innovation institutes and centers of excellence is also crucial. These institutions bring together government agencies, defense contractors, solutions providers, and research institutions to drive innovation.

The DoD should establish data sharing protocols and standards that enable the secure and responsible sharing of relevant data among government agencies, defense contractors, and research institutions. This involves developing data governance frameworks, anonymization techniques, and data access agreements to facilitate data availability while ensuring privacy and security.

Initiating joint research and development programs that bring together government agencies, defense contractors, the private commercial sector, and research institutions is another key strategy. These programs can address common challenges and advance AI adoption in defense systems, focusing on areas such as AI algorithms, data analytics, cybersecurity, and human-machine teaming.

To facilitate technology transfer and commercialization efforts, the DoD can support the transition of AI technologies developed in research institutions, the private sector, or government agencies to defense contractors. This can involve providing guidance, resources, and incentives for technology transfer, licensing agreements, or spin-off companies.

As noted in response to Question 3, democratizing access to trusted and assured datasets is essential. Intellectual property rights, such as government purpose rights and common databases, would help foster and accelerate information-sharing and collaboration.

***8. 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/or operational defense systems?***

It is essential to establish clear expectations for assessing training data and models to prevent adversarial data injection and modifications. This involves developing a risk-based framework for the Independent Verification and Validation (IV&V) of AI in defense systems. Standardized approaches to evaluating AI risk should be created, focusing on mitigating adversarial exploitation during operations.

Research and experimentation programs should prioritize mitigating AI risks. This includes employing data quality techniques to ensure training data accurately represents real-world distributions, utilizing Run Time Assurance (RTA) approaches, and applying formal methods to prove the correctness of AI models. Additionally, enhancing trust in AI systems through explainability and other techniques is crucial.  For high-consequence development, including feedback mechanisms such as human review in-the-loop will be needed.

The rise of AI and digital solutions has led to the creation of a parallel digital supply chain. Like physical supply chains, the DoD can define specific digital supply chain security protocols that align with existing efforts such as NIST 800 and CMMC. Establishing guidelines and standards specifically addressing the security considerations of AI technologies within the Defense Industrial Base (DIB) is vital. These guidelines should cover secure data handling, secure model deployment, and continuous monitoring of AI systems to detect potential adversarial attacks.

The DoD should conduct comprehensive threat assessments and risk analyses to identify potential vulnerabilities and risks associated with AI technologies within the DIB. This includes evaluating the potential for adversarial exploitation, understanding the threat landscape, and assessing the potential impact on defense systems. Establishing continuous monitoring mechanisms is also recommended.

Furthermore, the DoD can partner with industry to establish security standards and guidelines specifically tailored to AI technologies within the DIB. These standards should address cybersecurity, data protection, and system integrity to ensure AI systems are resilient against adversarial exploitation. Additionally, partnering with industry and academia to provide training and awareness programs for the DIB workforce is essential. These programs should promote cybersecurity best practices, raise awareness about social engineering techniques, and foster a culture of security within the DIB.

## Acquisition, Policy, & Regulatory Environment

***9. 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 (https://rai.tradewindai.com/).***

The Department of Defense faces several challenges in the realm of AI governance, primarily due to a lack of consistent direction and standards. This inconsistency can hinder the effective implementation and oversight of AI technologies within the defense sector.

Export controls, designed to protect national security, often restrict the transfer of AI technology to foreign entities and countries. While these controls are crucial, they can also limit the Defense Industrial Base's (DIB) ability to collaborate internationally and innovate. Additionally, compliance with privacy and data protection regulations poses significant operational challenges for the DIB. These regulations are essential for safeguarding personal information but can complicate data handling and processing activities.

Ethical and legal considerations, such as addressing bias, ensuring transparency, maintaining accountability, and providing human oversight, are critical yet challenging aspects of AI governance. These issues necessitate robust governance frameworks to ensure that AI systems are developed and deployed responsibly. Furthermore, the process of accessing classified information and obtaining security clearances is both time-consuming and resource intensive. This requirement can impede the DIB's ability to engage in certain projects, thereby affecting overall efficiency and participation.

To address these challenges, the adoption of the Organisation for Economic Co-operation and Development's (OECD) definition of AI is recommended. The OECD's definition offers a comprehensive and widely accepted framework for understanding and discussing AI, which can provide a solid foundation for developing consistent governance standards.

***10. 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?***

Government-furnished secure cloud environments, platforms, and tools provided for DoD and IC programs have proven to be an effective strategy for supporting the DIB in transitioning AI for defense applications.

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

Unified expectations across services are crucial for the Department of Defense (DoD). As noted in response to question #1, ensuring data availability is a key component of this unification. Consistent access to data across all services will enable more efficient and effective operations.

Intellectual property protections and associated funding are essential to encourage private entities to invest in developing new models and training them for use in DoD systems and services. As highlighted in response to question #6, without these protections and funding, private sector investment in innovative technologies may be limited.

Flexible contractual structures, such as outcome-based versus cost-plus contracts, can provide significant advantages. This flexibility allows for more tailored and efficient agreements that can better meet the needs of both the DoD and its contractors.

The DoD should consider aligning with civil private equity and utilizing constructs such as In-Q-Tel to create new avenues of capital for emerging AI opportunities. This alignment can help bridge the gap between military needs and private sector capabilities, fostering innovation and growth in AI technologies.

Allocating and funding research and development (R&D) activities focused on AI technologies is another critical step. By incentivizing the Defense Industrial Base (DIB) to invest in internal AI R&D for defense applications, the DoD can ensure that cutting-edge technologies are developed and integrated into its operations.

Other Transaction Authority (OTA) agreements can streamline the acquisition process, providing faster procurement, reducing administrative burdens, and increasing opportunities for collaboration. These agreements can incentivize the DIB to invest in AI technologies by making the process more efficient and attractive.

The DoD can also structure contracts with specific incentives to encourage the DIB to invest in AI technologies. These incentives can be designed to reward innovation and successful implementation of AI solutions, further driving investment and development in this critical area.

Finally, democratizing access to trusted and assured datasets is vital, as noted in response to question #7. Intellectual property rights, such as government purpose rights, and the establishment of common databases would help foster and accelerate information-sharing and collaboration. This approach will ensure that all stakeholders have the necessary data to develop and deploy effective AI technologies.

***12. 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?***

Intellectual property protections are crucial for supporting the necessary private investment in model training and advancement, as noted in response to question #6. These protections ensure that companies can confidently invest in developing new technologies without fear of losing their competitive edge. Additionally, identifying pathways to leverage investments from international allies and partners in AI can significantly enhance our capabilities and foster global collaboration.

The Department of Defense (DoD) can accelerate alignment on data constructs, governance, and standards to support the flexible application of AI within open systems approaches. This alignment is essential for creating a cohesive framework that allows for the seamless integration of AI technologies across various defense applications. The Defense Industrial Base (DIB) requires access to large amounts of high-quality data to train AI algorithms effectively. However, ensuring the availability, quality, and security of this data can be challenging due to its sensitive nature.

Integrating AI systems into existing defense infrastructure and ensuring interoperability with legacy systems is a complex task. The DIB must develop standards and frameworks to facilitate the seamless integration and interoperability of AI technologies. This will ensure that new AI systems can work effectively alongside existing technologies, enhancing overall defense capabilities.

Several barriers must be addressed to achieve these goals, including data access and sharing, cybersecurity and resilience, ethical and legal considerations, workforce readiness and training, acquisition and procurement processes, and regulatory and policy frameworks. Overcoming these barriers will require a concerted effort from all stakeholders involved.

As noted in response to Question 7, democratizing access to trusted and assured datasets is essential. Intellectual property rights, such as government purpose rights, and common databases would help foster and accelerate information-sharing and collaboration. This approach will ensure that all parties have access to the data they need to develop and deploy AI technologies effectively.

Finally, evolving Cybersecurity Maturity Model Certification (CMMC) requirements and overlapping inconsistencies with the marking and handling of Controlled Unclassified Information (CUI) and proper data classification present additional challenges. Given that AI is heavily reliant on data, addressing these issues is critical to the successful implementation of AI technologies within the defense sector.

Finally, the DoD should consider how best to test for and identify hallucinations associated with Generative AI outputs.  For inexperienced or non-expert users, these outputs could be used as a source of truth with associated actions that would be counterproductive, or at worst, fatal.

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

Generative AI can significantly benefit smaller suppliers by providing a natural language interface to better understand regulatory requirements and other policies, especially when they lack in-house expertise. This technology can also support lower-cost information access across multiple DoD supply chain systems, improving the accuracy and timeliness of demand, supply, and material availability.

AI has the potential to revolutionize supply chain management by optimizing inventory levels and identifying potential bottlenecks or disruptions. It can automate order processing, track shipments in real-time, and provide recommendations for cost savings and process improvements. Additionally, Natural Language Processing (NLP) algorithms can automate the analysis of contract documents, identifying key terms, risks, and compliance requirements, thereby streamlining contract management.

Enhancing supply chain visibility is another critical area where AI can make a substantial impact. By analyzing real-time data from various sources, AI enables proactive monitoring, risk assessment, and mitigation. AI-powered systems can also automate compliance reporting, reducing manual effort and improving accuracy.

Furthermore, AI can assist in the qualitative analysis of proposals, contract novation, requirements traceability, and cost/schedule risk assessment. These capabilities ensure that the DoD can maintain high standards of efficiency and effectiveness in its operations, ultimately leading to better outcomes and enhanced readiness.