March 14, 2025

Mr. Faisal D'Souza
National Coordination Office
2415 Eisenhower Avenue
Alexandria, VA 22314

Email Submission: ostp-ai-rfi@nitrd.gov, *Document Number: 2025-02305*

Re: NDIA Comments on Development of an Artificial Intelligence Action Plan[1]

Dear Mr. D'Souza:

The National Defense Industrial Association (NDIA) appreciates the opportunity to provide comments on the request for information on the Development of an Artificial Intelligence (AI) Action Plan ("Plan") by the Networking and Information Technology Research and Development (NITRD) National Coordination Office (NCO).

NDIA is the nation's largest defense industry association, representing over 1,700 corporate and over 67,000 individual members from small, medium, and large contractors, a majority of which are small businesses. NDIA members design, manufacture, apply, and maintain the cutting-edge technologies, systems, and platforms that our armed forces rely upon to deter aggression and defend our nation and its interests. As such, our members' professional and informed views on this proposed rule reflect the complexity and nuance of the issues under discussion.

AI and Machine Learning (ML) are general-purpose technologies that can be leveraged across a wide range of use cases and offer tremendous benefits to society and national security. Today, major industries are utilizing AI to improve their product and service offerings to consumers, including everything from email spam filters to autonomous vehicles.

The U.S. Department of Defense (DoD) identifies AI as a technology with disruptive potential for defense capabilities and highlights it as a critical technology area for enhanced attention and investment. AI, ML, and autonomy are all poised to drive the military technological innovation needed to equip our warfighters with AI-enabled systems to improve the speed, quality, and accuracy of decisions in the field, which can provide the decisive advantage needed to deter or win a fight.

Winning the race to maintain the U.S.' technological competitive advantage requires deeper analysis of debates around the policies and authorities for these technologies. Getting the balance right will make or break whether the U.S. government (USG) can successfully buy and integrate new technology at speed and scale fast enough to preserve and, where necessary, expand the U.S.' technological competitive advantage.

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

NDIA offers the following areas for consideration for the AI Action Plan:

Promoting Government Use of AI

The opportunities for applying AI technologies are effectively limitless, and the government should prioritize making AI technologies easier to procure and deploy across all government missions, including the acquisition of commercial AI solutions using commercial purchasing authorities, terms, and conditions. The U.S. needs reliable AI that provides trusted and relevant answers to mission-specific questions. The Administration must prioritize data investments to coincide with AI tool procurement and deployment across government. To help industry tailor its recommendations for AI investments that will most effectively meet agency mission needs, the government should focus on the following areas:

- **Defining AI:** Artificial intelligence is a broad category that ranges from relatively straightforward data analysis and search functions to highly complex threat prediction capabilities. Setting a clear, common definition for how the government views AI as a technology enabler will allow businesses to provide clearer guidance for AI investments. The government should leverage existing work at the National Institute of Standards and Technology (NIST) to ensure harmonization across the AI landscape.

- **Utilizing existing laws:** It is essential to leverage existing technology-neutral laws and sector-specific regulations that already govern AI in the context of government procurement and cybersecurity policy. The Administration should reemphasize these frameworks, legal definitions, and agency authorities related to government procurement. AI is an evolving technology, but the application of statutory definitions to new technologies has been a constant practice. Existing legal definitions and implementing regulations in agency-specific legislation continue to apply to federal government IT systems.

- **Setting clear direction on which mission areas are the highest priority for leveraging AI:** Given the broad range of AI applications, it is crucial for agencies to provide clear guidance and demand signals on priority mission areas for AI investment. Indicating which areas are most important and ready for AI implementation will allow companies to direct their efforts towards solving critical national challenges. Agencies should incentivize innovation with AI in existing programs that require AI-driven processes and standards for acceptable AI system deliverables under contracts.

- **Ensuring access to commercial cloud resources:** Agencies should seek to leverage existing discount programs to ensure low cost for compute and inference services in future years. Computing power is essential for AI. Once the DIB and non-defense contractors integrate AI into their functions and processes, they cannot proceed without the higher level of computing. As airlines have done with fuel prices, the government should consider investing upfront and locking in today’s price for computing. Further, the government should assess its access to commercial cloud computing capacity at all classification levels and ensure it has access to the requisite level of processing capacity at the unclassified, secret, and top-secret levels to handle mission-critical training and inference workloads.

- **Leveraging commercial terms and conditions:** Accepting commercial data rights and customer-generated IP rights are the future of faster innovation. The Administration should encourage widespread adoption of standard commercial terms as much as possible and direct agencies to leverage commercial licensing terms of service for AI in harmonization with existing terms used across U.S. federal public sector commercial contracting of computer software (See FAR 12.212.) and standard commercial practices.

- **Focusing on buying solutions, not just AI:** The USG will not see a meaningful return on its AI investments buying discrete AI tools. Instead, the USG should buy integrated solutions tied to clear mission outcomes. These solutions may include many different AI components, but none of them will achieve mission outcomes on their own. The distinction between solutions and tools is important. Every AI component will require significant updates to maintain its usefulness – or need to be swapped out altogether for a different component – while the broader solution may achieve successful mission outcomes for years. Shifting to an outcomes-focused posture will provide three key benefits. It will: (1) simplify the USG's requirements; (2) increase optionality in the selection of tools and partners; and (3) reduce mission risk by focusing on pre-integrated solutions that can be deployed quickly and securely.

- **Provide accessibility to high-quality, curated training data:** Robust, high-quality data is a necessity for AI developers. Publicly available training data has the potential to create issues including IP infringement, prompt injection, or other concerns. The government should create a repository of such data and create initiatives to share such data responsibly while maintaining security and privacy standards.

Removing Barriers to Expand the Use of AI

Meeting the needs of our national imperatives depends upon a diverse set of industry partners with access to critical technology. The government should work with industry to identify and remediate roadblocks where government policies and regulations unnecessarily slow the adoption of AI. Government acquisition processes must be modernized to match the pace of technological change and enable more efficient procurement of commercial AI solutions. Areas where barriers should be removed include the following:

- **Shorten and simplify the ATO process:** One of the largest barriers to efficiently introducing new AI capabilities to the USG is the Authorization and Accreditation process to receive an Authority to Operate (ATO). Getting a traditional ATO can take over a year at a substantial cost, which can be very burdensome to small businesses and a barrier to rapidly delivering relevant software capabilities to agencies. Two very prominent examples are FedRAMP and IL4/5. To be clear, these certifications are necessary and important. But they are unnecessarily long and laborious, often preventing innovative startups from adding value to the USG, if they even try. The two principal reasons to reform these processes are: (1) they can take a year or more to complete, stifling progress and dissuading new companies from serving the U.S. Government; and (2) they arbitrarily require an agency to sponsor a certification before the process can even begin, despite the cost and burden borne almost exclusively by the company seeking the certification.

To address these issues, it will be necessary to deeply reevaluate the ATO process and identify where improvements can be made. Initially, however, NDIA proposes three key changes: (1) all certifications can be initiated and undertaken by the company seeking one without agency sponsorship (but agencies will still be responsible for the final certification); (2) authorizing officials should be measured on how effectively they support requirement sets and incentivized accordingly; and (3) agencies should continue to push for greater utilization of reciprocity within the ATO process. The result of these changes will be a net increase in the critical AI companies that are ready and able to serve the USG with fast and efficient delivery of innovative capabilities critical to our national security.

- **Do not unnecessarily block AI applications by default:** To win the AI competition with the People's Republic of China, the USG must avoid reactively banning new AI models when they are released. This prevents the USG from doing two key things: (1) understanding, and if necessary, defending against their true risk factors, which cannot be accomplished without directly engaging with the models; and (2) leveraging the most advanced capabilities available when even incremental performance gains in a frontier model can make a national security mission more successful or secure. Put simply, reflexively banning AI models by default puts the U.S. at a competitive disadvantage.

  NDIA recommends a policy that emphasizes broad AI use and security. There is no doubt that certain foreign-developed AI models present security challenges, and some may not make sense to use in, or for, USG systems at all. But there are known – and proven – tools and methods to manage AI security risks while still leveraging a model's capabilities. Therefore, the default policy of the USG, including all agencies, should be to use all available AI models to address mission requirements, while taking prudent steps to deploy those models securely and protect U.S. intellectual property. To that end, the USG may consider standing up a function to rapidly recreate open-source models with standard security controls, enabling the trusted deployment of AI solutions across missions of national importance. This approach would be further enhanced with the participation of select international partners. In addition, the full assessment of new AI models would enable the ability to recognize and develop counter-AI. Like the Intelligence Community shifted their posture from "Need to Know" to "Need to Share" after 9/11, we recommend an analogous shift from "AI Can't Be Trusted" to "AI Must Be Used." The USG must use every AI tool at its disposal without security being an unnecessary impediment.

- **Increase access to chips and other technologies:** The ever-greater reliance on computing power to operate complex systems depends on access to chips and other key components. Large-scale commercial entities have the resources and buying power to monopolize this market if they choose or if, at any point, supplies become substantially limited. The Department should work to ensure that these technologies remain available to the defense industrial base to help meet mission needs as required.

- **Promote open-source and AI:** NDIA members find the lack of open models that enable free and permissive use concerning. All current major commercial open models contain significant license restrictions that explicitly deny the use of their models for defense applications, and NDIA recommends DoD negotiate with the model creators to remove the “defense application” restriction. This is a major issue for the DIB and DoD equities. In addition, most models advertised as ‘open-source’ models are merely ‘open-weight’ models (e.g., the model weights are available, but the data and source code used for training these models are not visible), which makes it more difficult to investigate the integrity of the models themselves. The government should work with model developers to provide truly open-source, secure models to allow for innovation and AI-enabled system development.

- **Protect the hardware supply chain:** The future of the government’s computing supply chain is vulnerable due to the sheer amount of training compute resources. Given the private sector’s rapid adoption of this technology, the government may compete for scarce hardware resources in the future. To ensure the government’s ability to deploy real-time AI capabilities, particularly Gen AI capabilities, we must increase investment in Gen AI computing capacity. Further, the government should also increase its access to this critical hardware by leveraging commercial cloud capabilities at all classification levels. Additional investments in tactical (3U, 6U, etc.) compute resources beyond the GPU architecture may also be necessary to take advantage of the proliferation of Gen AI solutions across the DIB and non-defense contractors.

Supporting Partnerships, the AI Workforce, and New Entrants

- **Leverage mentor-protégé programs:** The USG should create mentor-protégé programs that allow existing contractors to bring expertise in meeting agency customer expectations while leveraging small and innovative company capabilities. To be impactful at scale, such programs must allow mentor companies to have a number of protégés concurrently, and that number should take into consideration the size/scope of the mentor company. The current blanket limit of three protégés per mentor for some programs greatly reduces the potential impact of the program.

- **Foster partnerships:** Given the broad range of AI applications, it is crucial for agencies to provide clear guidance and demand signals on priority mission areas for AI investment. Indicating which areas are most important and ready for AI implementation will allow companies to direct their efforts towards solving critical national challenges. Agencies should incentivize innovation with AI in existing programs that require AI-driven processes and standards for acceptable AI system deliverables under contracts.

- **Consider new consortiums:** The establishment of agency-industry consortiums will enable relationship development and collaboration on relevant issues. The Artificial Intelligence Safety Institute Consortium (AISIC) housed under NIST is a good example that unites AI creators and users, academics, government and industry researchers, and civil society organizations in support of the development and deployment of safe and trustworthy AI.

- **Increase use of SBIRs, OTAs, and BAAs for AI:** The USG should provide resources for new entrants to understand how to work with federal agencies and provide access to training data for AI developers. Smaller companies, particularly small and sophisticated software companies, may avoid partnering with the USG because of the antiquated data rights rules in the FAR and DFARS. Such resources should be made more flexible for the acquisition of AI tools in order to attract these new entrants. Additionally, contracting and agreements officers using flexible contracting vehicles for AI should be trained in adopting commercial business practices and contract terms to ease the barriers for all companies seeking to offer their AI solutions to the government.

- **Ensure transparency in contracting costs and assistance for small businesses:** Without knowing the full costs of contracting, it can be difficult for industry partners, especially small businesses and nontraditionals, to make a fully informed business decision of whether to conduct business with the USG, which can become a large barrier to entry. For example, the existing requirement for DoD contractors to meet cybersecurity standards under NIST SP 800-171 and the coming requirement for non-defense contractors under the proposed FAR rule for Controlled Unclassified Information (CUI) impose high initial costs and annual recurring costs on contractors. DoD contractors must expend additional funds for third-party assessment and certification under the Cybersecurity Maturity Model Certification (CMMC) program. Besides providing transparency to new entrants of what it costs to contract with the government, Congress and the Administration should consider providing assistance through the form of tax credits and loan guarantees to help attract small businesses with innovative solutions.

- **Enable flexible facility security clearance on-ramps:** The USG should provide security clearances for AI developers who work across multiple programs at various classification levels. As we work to stand up AI infrastructure capabilities to serve the USG in classified environments, we are often limited in our ability to provide services in classified domains due to limited cleared staff billets. Once the agency tests a capability at the unclassified level, having more cleared personnel across the DIB will enable agencies to move the solution to a classified fabric mission use.

- **Build the AI workforce pipeline:** Establishing priority lists of AI subspecialties to share with academia and industry would help accelerate research focus and academic development to support a sustainable AI knowledgeable workforce.

Expanding Access to Innovation by Respecting Private Industry IP and Data Rights

Developing and deploying AI-enabled defense systems often involves collaboration between multiple entities, including government agencies, defense contractors, new entrants, and research institutions. Determining ownership, sharing intellectual property (IP) rights, and addressing copyright, trademark, and patent issues in collaborative projects is highly complex. NDIA recommends that the government establish a collaborative process to work with industry to develop contracting mechanisms and acquisition strategies that respect and protect privately developed IP to the greatest extent possible and focus on acquiring only those technical data deliverables and license rights necessary to accomplish the specific definitive goals of the government at hand. Respecting the private sector's IP rights and more closely aligning with commercial practices will incentivize investment and provide the government with greater access to the most advanced technological innovations.

Utilizing AI to Improve Acquisition and Procurement Processes

AI, specifically Gen AI, has demonstrated its ability to accelerate productivity in nearly all industries. Acquisitions will benefit from accelerated insights, while supply chain management will benefit from integrated data insights and analytics that provide efficiencies. The following are several considerations for utilizing AI to improve the acquisition and procurement processes:

- AI has the potential to augment the entire acquisition cycle. AI-enabled proposal writing, cost estimating, schedule planning, supplier control, compliance planning, model development, and artifact generation for regulatory compliance are all areas where having agency standards and/or example models in place that could be shared with the DIB could have a dramatic positive impact. The use of AI in this process could fundamentally change acquisition products and evaluation activities. User training will also be critical to ensure that AI users understand the capabilities and reliability of their AI tools and remain responsible for the accuracy of AI-generated content.

- Contractors should be informed if AI products were used in the creation of RFP materials or if they will be planned for use in the evaluation. The government should also disclose when it's using AI for source selection or another way in the market research or other proposal processes.

- To promote more accurate models and build new AI tools, DoD will need to improve its data infrastructure and overall data collection efforts. Insufficient data collection, labeling, and storage is a critical barrier to exploring how AI capabilities could promote efficiency within the acquisition lifecycle. DoD must continue to encourage the electronic collection of data and emphasize that an agile architecture will allow it to rapidly adapt to changing requirements and user needs.

- AI can assess and identify correlations and insights in large data sets that can support more effective decision-making, identify compliance hot spots, and allow for a more efficient allocation of resources.

- The government should support innovative advancements while leveraging existing commercial technologies.

- The government should focus on leveraging cloud-based solutions at all classification levels.

- Streamline the FedRAMP authorization process by leveraging tools that automate evaluation and risk identification. For example, AI can be used in tools that enable true continuous monitoring, reporting, and threat mitigation, thus enhancing cybersecurity across the enterprise.

Conclusion

NDIA and its membership appreciate the government's desire to promote a strong, dynamic, and robust defense industrial base. If you have any questions related to these comments, please contact Michael Seeds at mseeds@ndia.org.

Sincerely,

National Defense Industrial Association