About the Aerospace Industries Association:

For over 100 years, the American aerospace and defense (A&D) industry has shaped the world around us. With more than 2.2 million shared employees and generating $425 billion in economic value, we are critical to the health of the U.S. economy and serve as a seamless, fundamental part of daily life. Now more than ever, it's vital that our collective industry has a strong voice speaking on its behalf.

The Aerospace Industries Association has been that voice since 1919. Our work as an advocate and leader is essential to shaping policy, shedding light on the industry's impact, and fortifying its future. Together with our member companies, our advocacy influences: effective federal investments; accelerated deployment of innovative technologies; policies that enhance our global competitiveness; and recruitment and retention efforts that support a capable and diverse 21st century workforce.

We are pleased to submit the following comments in response to the Request for Information: Development of an Artificial Intelligence Action Plan posted as Federal Register Number 2025-02305.

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.

Recommendations on Intellectual Property protections:

To ensure the successful deployment of AI systems, it is crucial for the government and industry to establish clear data ownership rules for datasets where both parties have made investments. This includes creating guidelines for data sharing agreements and intellectual property rights for derived data. The Aerospace Industry Association (AIA) emphasizes the importance of defining processes to make government datasets accessible for model training while addressing data security. In addition to government dataset availability, considerations on how and if to make third-party datasets that are procured by the government available for external use. Additionally, regulations must be established to determine the ownership of resulting AI models, recognizing the value of both government-supplied data and private entity investments. This approach will incentivize investment in model training and ensure that proprietary information is protected.

Establishing model ownership rules is essential when training data is owned wholly or partially by the government. This includes creating licensing agreements for joint

ownership and guidelines for the commercial use of government-trained models. The AIA advocates for recognizing the need for investment to train models and the associated intellectual property protections that will incentivize such investment. Regulations should be structured to acknowledge the contributions of both parties, ensuring that proprietary information is protected and that clear standards are established for AI system outputs as deliverables. This approach will support the ongoing development of AI solutions within the Department of Defense (DOD) and the Defense Industrial Base (DIB).

Recommendations on Certifying AI systems for use:

The government should develop comprehensive frameworks for the verification and validation (V&V) of AI capabilities. These frameworks should include standardized approaches to evaluating AI risk, creating playbooks of controls, Concepts of Operations (CONOPS), architectural frameworks, and design patterns to mitigate risks. The DoD should invest in developing a framework for the Independent Verification and Validation (IV&V) of AI in defense systems, ensuring that AI systems are reliable, safe, and effective. This includes establishing test ranges, simulation environments, and evaluation criteria to validate the performance and suitability of AI technologies.

The frameworks for verification and validation should fall into two main categories:

1. Development Assurance (Learning Assurance): This category focuses on ensuring the functional safety of AI during its development phase. The current approach, as proposed by the software and systems engineering community, includes 60 additional accomplishments for AI functions related to development and learning assurance. However, these methods are not scalable to real-world problems, particularly for large language models and deep neural networks. Therefore, it is crucial to develop scalable mathematical methods applicable to these advanced AI models.
2. Verification and Validation of Safe Behavior: This category emphasizes ensuring the safe behavior of AI systems through architectural means, such as implementing monitors and guard rails. This approach can help in continuously verifying and validating AI systems' safety in real-world applications.

Verification and validation of AI capabilities should not be considered a one-time, pre-deployment event. Instead, the frameworks should include methods for continuous monitoring, data collection, and user feedback gathering for fielded AI systems to monitor for data and model drift. This approach ensures that AI systems remain effective and reliable over time. Continuous retraining and model refinement based on the data

collected will help address any changes in the operational environment and maintain the accuracy and performance of AI systems.

The framework should also consider the requirements and design phases of AI systems. This includes providing requirements for model and dataset selection, such as identifying forbidden countries or data sources for government workloads. Additionally, the framework should include system documentation and review requirements, such as the AI Bill of Materials (AI BoM), which lists all components involved in the creation and deployment of AI systems. This approach is similar to the Preliminary Design Review (PDR) and Critical Design Review (CDR) processes used in traditional systems engineering.

The framework should include different design assurance levels based on the criticality of the workload, similar to the Design Assurance Levels (DAL) in DO-178C. For mission-critical AI workloads, more stringent requirements for model and data selection, increased model transparency, and tighter review processes are necessary. This approach ensures that high-consequence AI systems are developed and deployed with the highest standards of safety, reliability, and performance.

The framework should also consider the risk management process, including identifying the government entities responsible for providing risk assessments and Authorization to Operate (ATO) for AI systems on government workloads. This involves developing a risk-based framework for the Independent Verification and Validation (IV&V) of AI in defense systems, ensuring that AI systems are resilient against adversarial exploitation and other risks. Establishing clear expectations for assessing training data and models will help prevent adversarial data injection and modifications.

The DoD should develop standard feedback loop processes to support contractor feedback on deployed model performance and operational update processes for contractor-provided model updates. These processes will enable continuous improvement of AI systems by incorporating real-world performance data and user feedback. Additionally, they will facilitate efficient usage of networks and dataset classification, ensuring that AI models remain accurate and effective over time.

The government should consider building, procuring, or certifying foundational AI models that can be used by industry. These models should be developed with consideration of whether they are open source or proprietary. By providing access to high-quality foundational models, the government can support the development of AI solutions across various sectors, ensuring that these models meet the necessary standards for security, reliability, and performance.

The DoD should recommend utilizing an "AI Use Case Catalog" at the US government level to track AI development across various government agencies. This catalog would facilitate the reuse of both models and data, promoting efficiency and reducing redundancy. By maintaining a comprehensive record of AI use cases, the government can identify opportunities for collaboration and leverage existing resources to enhance AI capabilities.

Recommendations on Data Availability and Security:

To accelerate and maximize the adoption of AI, it is essential for the U.S. government to make its datasets accessible to contractors. The DOD should define processes to ensure secure access to these datasets while addressing data security concerns. This initiative will enable contractors to leverage high-quality data for model training, fostering innovation and enhancing the overall effectiveness of AI systems.

The DoD should invest in creating and maintaining digital twins and simulation environments that can be accessed by contractors. These environments provide valuable opportunities for experimentation, testing, and validation of AI systems in realistic scenarios. By making these resources available, the government can support the development of robust and reliable AI technologies.

To ensure the efficient and effective use of government-owned datasets by contractors, it is crucial to include comprehensive metadata. Metadata provides essential information about the dataset, such as its origin, structure, and usage guidelines. This enables contractors to understand and utilize the data more effectively, leading to better AI model performance and outcomes.

The government must establish policies and techniques to ensure that datasets provided by contractors, universities, and government entities are accurate, unbiased, and free from data poisoning. This includes implementing data quality assurance processes, conducting regular audits, and employing advanced techniques to detect and mitigate biases and data manipulation. Ensuring the integrity of datasets is critical for developing trustworthy and reliable AI systems.

Ensuring data privacy and security throughout the AI lifecycle is paramount. This includes robust measures for data collection, storage, processing, and sharing. The Aerospace Industry Association (AIA) emphasizes the importance of addressing cybersecurity implications by establishing requirements around data governance, testing, transmission, and ownership. High-quality data is essential for training and operating AI systems effectively, but the data supply chain can be vulnerable to manipulation, tampering, or contamination. Therefore, the DOD must establish mechanisms to ensure the integrity and

quality of data used in AI systems. 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.

Recommendations on Export and Import of AI systems:

The government must continue to refine export controls for dual-use technologies, especially where it would be advantageous to involve foreign entities. Export controls are designed to protect national security but can also limit the DIB ability to collaborate internationally and innovate. The AIA recommends that the DoD consider a unified approach to export classification for published datasets, establishing clear expectations on how data is provided, accessed, shared, assessed, related, and owned. This approach will facilitate the deployment of AI systems while ensuring that sensitive technologies are protected. Additionally, the DoD should invest in interoperable, federated infrastructure, advance the data, analytics, and AI ecosystem, and improve foundational data management. By refining export controls, the U.S. can balance the need for security with the benefits of international collaboration.

The government should refine the rules associating the classification of data sets to clarify the classification of the resulting model. For instance, if the data set is subject to the International Traffic in Arms Regulations (ITAR), it is crucial to determine whether the final model is also ITAR-compliant. The AIA highlights the need for clear regulations to determine the ownership of resulting AI models, recognizing the value of both government-supplied data and private entity investments. Additionally, the DoD should consider the classification of aggregate information derived from disparate datasets, as the aggregate information might be classified even if the constituent datasets are not. This approach will ensure that AI models developed using classified data sets are appropriately managed and protected.

Recommendations on investments to increase usage of AI in small businesses:

The government should continue to fund specific Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs focused on translating commercial AI capabilities into defense applications. These programs provide essential support for small businesses and non-traditional defense contractors, fostering innovation and enabling the development of cutting-edge AI technologies for defense purposes.

Recommendations on Simplifying the Certification Process:

The single biggest hurdle to introducing new AI capabilities into the U.S. Government is the certification process. Known as "A&A" - Authorizations and Accreditation - the two most 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 U.S. Government, 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; (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, we propose two 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 (i.e., the *value* they provide to U.S. Government missions) and incentivized accordingly. The result of these changes will be a net increase in the critical AI companies ready and able to serve the U.S. Government, dramatically increased innovation, and fast and efficient delivery of capabilities critical to our national security.

Recommendations on Pro-Use AI Policies:

To win the AI competition with China, the U.S. Government must avoid reactively banning new AI models when they're released. This prevents the U.S. Government 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; (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 puts the U.S. at a competitive disadvantage.

We recommend 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, U.S. Government 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, we recommend the default policy of the U.S. Government, including all Executive Branch Agencies, 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 U.S. Government 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.

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 U.S. Government must use every AI tool at its disposal without security being an unnecessary impediment.

Recommendations on Buying Solutions, Not AI:

The U.S. Government will not see a meaningful return on its AI investment by continuing to buy discrete AI tools. Instead, we recommend the U.S. Government focus on buying 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 also important because 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 U.S. Government's requirements; (2) increase optionality in the selection of tools and partners; (3) reduce mission risk by focusing on pre-integrated solutions that can be deployed quickly and securely.

Recommendations on forums for industry and government collaboration on artificial intelligence deployment inside the DOD and DIB:

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 crucial. This collaboration will foster innovation and promote the development of trustworthy AI systems.

The DoD should focus on assessing and advancing the digital maturity of the DIB, particularly at lower tiers. Given that AI and Gen AI are heavily dependent on a solid data foundation, gaps in technology maturity and investment capacity can significantly limit the ability of the full DIB to take advantage of AI. Establishing programs that enable lower-tier suppliers to benefit from AI investments will ensure that all levels of the DIB can leverage advanced AI technologies.

Investing in AI education and training for universities and the workforce, both in the private and public sectors, is essential for building a robust AI ecosystem. The DoD should establish and invest in university academic programs to train 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.

The rapid advances in AI capabilities have the potential to disrupt the DoD and DIB workforce. The DoD should establish programs to provide training that will enable employees at all levels of the DIB to safely and effectively use AI. This training will help the government workforce become citizen AI users, understanding the capabilities, limitations, and potential impact of leveraging AI technology.

The DoD should consider leveraging existing Innovation Hubs. These hubs provide valuable resources and support for the development and deployment of AI technologies. By utilizing these innovation centers, the DoD can foster collaboration, accelerate innovation, and enhance the overall effectiveness of AI initiatives.