The Honorable Eric Fanning
President & Chief Executive Officer
Aerospace Industries Association

AI Insight Forum – National Security
U.S. Senate
Wednesday, December 6, 2023

Majority Leader Schumer and members of the Senate, thank you for inviting me to appear today. For over 100 years, the Aerospace Industries Association (AIA) has advocated for America's aerospace and defense (A&D) companies and the more than 2.2 million men and women we employ. Our members are America's leading manufacturers of defense aircraft and equipment, service providers, and suppliers of all sizes. In 2022, the industry generated $418 billion in economic value, representing 1.65 percent of total U.S. gross domestic product. AIA serves as a bipartisan convener, bringing people together to find consensus on topics important to our industry, like effective federal investments and the adoption of policies empowering our defense industrial base – and our country – for the 21st century and beyond.

Artificial intelligence (AI) is poised to reshape the way our world operates, and this is especially true for national security. Whoever leads in the development of AI technology and the establishment of a regulatory framework to govern the use of that technology today will likely govern the world's use of this technology well into the future. Therefore, it is critical from a national security perspective, as well as an economic competitiveness perspective, that the United States maintain our leadership in AI — becoming the global gold standard, just as the Federal Aviation Administration is for aviation safety, for instance.

As I testified in September at the first AI Insight Forum, the A&D industry focuses on five initial focal points from which to consider this discussion: the balance between regulation and innovation; data rights and management; federal procurement; our workforce; and near-term national security threats. The A&D industry has a long history of using AI to increase organizational effectiveness and efficiency and to deliver capabilities to customers. Examples include satellite battery monitoring technology that utilizes machine learning algorithms to allow ground control operators to proactively conduct maintenance actions that provide longer vehicle life, as well as AI models that provide more efficient threat identifications to the intelligence community.

The historical usage of AI within A&D has been supported by a set of expectations mutually developed between the industrial base and government regulators. One example of this collaboration is a revised version of Department of Defense Directive 3000.09, "Autonomy in Weapons Systems," that was released on January 25, 2023, which superseded the version released in 2012. As a regulatory framework is established, industry requests that the government consider the continuation of the historical model of existing purchasing agencies (such as the Department of Defense or the Federal Aviation Administration) and their customers to working

together to define regulatory expectations for AI. This model has proved to allow for those most familiar with the opportunities and concerns related to AI to collaboratively establish guardrails that balance the needs for protection from harm while allowing for rapid innovation. In any case, government regulators must be empowered with the tools and resources needed to protect safety, privacy, and American values, while not hindering American competitiveness globally.

Protection from harm is a primary concern of the A&D industry. In order to apply appropriate controls to AI implementation, U.S. policy should define possible levels of harm that should be defined by standards and tailor any testing, certification, and regulatory regimes appropriately. For instance, a standard could specify the level of harm as low, medium, high, or extreme based on the potential impact of the AI system on human lives, property, or the environment. Once a level of harm is identified, appropriate testing, verification and validation, ongoing human oversight, and governance requirements can be applied to identify and mitigate risks.

Advances in AI capability will require massive inputs of data — and accordingly, a frank discussion on data rights as it applies to national security uses. The government holds many such datasets, and the U.S. government should consider approaches to make such datasets available for model training. To do so, regulations must define ownership of resulting models in such a way that recognizes the value of the government provided data as well as the investment by the private entity with associated ownership of the model. Controlled access and classification may pose barriers to effectively harnessing AI, so government agencies should consider which data to provide with a focus on availability of datasets, relatability between datasets, and constituent data element quality. The private investment in training a model can be significant, and establishing ownership of models that have been trained with government data will create confidence in the defense industrial base that their investments in model training can be recouped. This will also incentivize the private sector to innovate and improve the AI models for the benefit of the A&D industry and the nation.

Establishment of AI governance standards can provide assurance that AI is being developed and deployed safely and effectively. Defining roles and responsibilities between providers and purchasers is crucial to reducing redundant activities while ensuring that proper risk management is applied to the system in question. Additionally, establishing accountability and transparency mechanisms can enhance trust and confidence in the AI systems and their outcomes.

With the global race to develop AI being partially throttled by available investment, it will be crucial to create an open environment where the U.S. and our allies can collaboratively work on developing AI models. This will require a well-defined regulatory landscape that allows for import and export of data, models, and test results that will protect the United States' interests while allowing for mutual investments with partner nations.

For the U.S. government, implementing updated data rights standards, coordinating with allies and partners, and acquiring AI technologies developed by industry will ultimately require reforms to the federal procurement system. This system already struggles to meet 21st century demands with, for example, the acquisition of software. AI will undoubtedly bring a whole new

set of challenges for procurement policy. The government must be prepared to keep pace not only with the U.S. private sector, but with a global effort to advancing the use of this technology.

All of this will require a capable, qualified workforce — not only engineers and scientists, but also manufacturers, including highly-skilled technical manufacturing jobs, and not only within the private sector and industry, but also within the government. As AI represents a new way of working with new tools, new expectations, and new processes, developing an AI-capable workforce will require investment at the primary and secondary educational levels as well as retraining for current A&D workforce members. To achieve this goal, we must support the development of additional training programs that enable the current and future A&D workforce to take full advantage of the possibilities of AI. For instance, curriculum should be developed that addresses AI ethics, data science, machine learning, and human-AI interaction that would equip the A&D workers with the necessary skills and knowledge to design, develop, and deploy AI systems in a safe and effective manner. On another level, we must consider reforming our immigration system and take advantage of talent that wants to come to the United States to work on these technologies.

None of this will take place in a vacuum. The global security environment will surely shape this regulatory framework, and it will not wait while Congress develops and implements a regulatory framework to protect American citizens, American businesses, American intellectual property, and our nation as a whole. It should be our goal to be the standard bearer and gold standard that shapes the global dialogue. This inherently requires working with our allies and partners to stay ahead of potential adversaries, and thus, establishing the export control protocols that enable this coordination and collaboration. However, it will also require the broader establishment of international norms — and we must lead this conversation. For national security applications, the consequences of AI are tremendous; AI technology has the potential to drastically change the way wars are fought, with many benefits, but also many areas of concern. The landmark agreement between the United States and China announced on November 15, which banned the use of AI in autonomous weaponry, such as drones, and in the control and deployment of nuclear warheads, is a welcome step and a prime example of the types of conversations with which the United States and other countries will continue to wrestle.

The A&D companies represented by AIA share Congress' enduring commitment to national security and the defense of the American way of life. The government has a willing partner in our members to address these challenges, accelerate innovation and acquisition, and set the United States on a stronger course for a more secure future.

In closing and on behalf of AIA and our members, I thank you for your time and consideration of these matters. As always, AIA is available to address any questions or concerns the Senate has now and in the future.

###