Second Front

Use of AI and LLM Attestation

Use of Artificial Intelligence and Large Language Model Attestation

Please complete this form by providing sufficient information to provide an authorizing official insight necessary to adjudicate the risk of artificial intelligence in DAF-approved applications.

Artificial Intelligence

1. **Does your Application employ artificial intelligence and/or machine learning?**

□ Yes
□ No

2. **Does your Application employ machine learning?**

□ Yes
□ No

Type of AI

□ Predictive Analytics
□ Machine Learning
□ Deep Learning
□ Natural Language Processing
□ Computer Vision
□ Reinforcement Learning
□ Ensemble Model
□ Generative AI

Machine Learning

If you selected "yes", your Application employs machine learning, complete the following questions. If not, disregard this section and proceed to Type of AI.

1. **Specify the Model Type**

□ Supervised Machine Learning
□ Unsupervised Machine Learning
□ Reinforcement Machine Learning

2. **Are you using a foundational pre-trained model?**

□ Yes
□ No

3. **Have you done additional training on the model?**

□ Yes
□ No

Machine Learning Security

1. **Is customer data fed back into the model?**

□ Yes
□ No

2. **What type of threat modeling was performed?**
3. **Was vulnerability scanning performed? What tools were used?**
4. **Was red teaming conducted? Who conducted the testing and what were the conclusions?**
5. **How does the application prevent spilling data in the form of an output?**

□ **I verify that this application has considered and addressed the OWASP Top 10 for LLMs and Generative AI Apps.**

Types of AI

If you selected “no”, your Application employs machine learning, complete the following question. If not, disregard this section and proceed to the Business Case.

- □ Process Automation
- □ Advanced Analytics

Computational Approach

1. **Please provide a description of the computational approach to your implementation of AI.**

Business Case

1. **Why does your application require AI?**
2. **What use case(s) are addressed by AI and what value is expected to be realized?**

Architecture

1. **Please provide a high-level depiction of the AI application architecture.**

Department of Defense AI Requirements

Explain how the application conforms to the DOD’s Ethical Principles for Artificial Intelligence.

1. Responsible. DoD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.

2. Equitable. The Department will take deliberate steps to minimize unintended bias in AI capabilities.

3. Traceable. The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedure and documentation.

4. Reliable. The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life-cycles.

5. Governable. The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.