OFFICE OF THE CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-9010

Statement on DoD's Compliance with M-24-10 and Transparency of AI Use

Per the Advancing American AI Act, the Department of Defense (DoD) is exempted from the Federal government's Artificial Intelligence use case inventory reporting requirement. However, we remain committed to transparency and are proactively addressing the requirements of the Office of Management and Budget (OMB) Memorandum M-24-10 by identifying potential rights- or safety-impacting AI use cases, and ensuring each use case's full compliance with the mandated AI risk management practices. The Chief Digital and AI Officer (CDAO), the Department's Chief AI Officer, (CAIO) will not, at present, be issuing any waivers for these practices, nor does the Department have any waivers to report. By January 10, CDAO plans to have thoroughly verified that this path toward compliance is in line with DoD's use of AI under M-24-10. Forthcoming updates on this work can be found at ai.mil.

To learn more about CDAO's steps to get in compliance with M-24-10, please see our compliance plan, published on September 24, 2024. To date, specific actions we have taken include:

- Regularly convening the CDAO Council, the DoD's AI governance body, to coordinate AI activities across the Department and address associated risks.
- Developing Department-wide guidance for implementing and certifying compliance with all minimum risk management practices in M-24-10 and the recently released National Security Memorandum (NSM-25) on AI.
- Ensuring the Department maintains an internal AI use case inventory, in line with requirements for other federal agencies, by building an initial list of AI use cases and conducting sustained dialogue across DoD to ensure the application of M-24-10 risk management practices. This effort includes engaging in the interagency effort to bring Food and Drug Administration-approved medical devices into compliance with M-24-10.
- Co-chairing the White House Chief AI Officer Council Working Group on Risk Management, which is producing a version of the DoD's Responsible (RAI) Toolkit tailored to help Federal Agencies leverage existing resources across the interagency to comply with M-24-10 and NSM-25 minimum risk management practices.

As a global leader in technological innovation, the DoD remains at the forefront of responsible AI adoption. Some examples include:

- Publicly releasing the DoD AI Ethical Principles and DoD RAI Strategy and Implementation Pathway.
- Releasing and regularly updating the RAI Toolkit. The RAI Toolkit provides a centralized process that identifies, tracks, and improves alignment of AI projects to RAI best practices and the DoD AI Ethical Principles, while capitalizing on opportunities for innovation.

- Publishing resources under the Joint AI Test Infrastructure Capability (JATIC) program, which develops publicly available software products for AI testing and evaluation (T&E) and AI assurance. In addition to open-source software, the JATIC program has developed a set of T&E frameworks aimed at building trust in AI-enabled systems in the Department.
- Providing guidance for the responsible fielding of generative AI through CDAO's "Guidelines and Guardrails to inform the Governance of Generative AI" to help DoD Components assess, identify, and proactively address risks that arise as these tools are procured, developed, and deployed. A forthcoming GenAI toolkit will provide additional resources to the Department in this area.
- Expanding RAI practices beyond the United States by convening the Partnership for Defense, an event that brings together partners and allies to discuss foundational issues in the responsible use of AI.

As AI capabilities become more widespread, the DoD remains committed to transparency, continuous improvement, and responsible technological advancement. CDAO will continue to lead and support the Department's compliance with Federal AI policy, including M-24-10, and adoption of effective AI governance and risk management.