



CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICER

9010 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-9010

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Department of Defense Compliance Plan for Office of Management and Budget Memorandum M-24-10

References: (a) OMB Memorandum M-24-10, “Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence,” March 28, 2024.
(b) OMB Memorandum M-16-21, “Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software,” August 8, 2016.
(c) U.S. Department of Defense, “Responsible Artificial Intelligence Strategy and Implementation Pathway,” June 2022.
(d) Executive Order 14110, “Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” October 30, 2023.

The Office of Management and Budget (OMB) Memorandum M-24-10, reference (a), directs the Department of Defense (DoD) to submit to OMB and post publicly either a plan to achieve consistency with OMB M-24-10, or a written determination that the Department does not use and does not anticipate using covered artificial intelligence (AI). As the DoD’s Chief AI Officer (CAIO) in accordance with Section 3.a.i of reference (a), the DoD Chief Digital and Artificial Intelligence Officer (CDAO) submits this memorandum, which comprises the Department’s compliance plan for reference (a) and conforms with the instructions provided by OMB.

While many of the DoD’s ongoing activities meet the requirements established in reference (a), OMB’s memorandum has prompted the Department to adapt certain existing processes, such as budget processes, to enable compliance. Additionally, to ensure consistency with minimum risk management practices for safety-impacting and rights-impacting AI activities (collectively referred to as “covered AI” activities), CDAO will develop DoD-wide guidance for complying with minimum risk management practices and requesting waivers for covered AI use cases.

1. Strengthening AI Governance

The CDAO Council serves as the Department’s AI governance body in accordance with Section 3.a.ii of reference (a), coordinates AI activities across the DoD, removes barriers to the use of AI, and addresses associated risks. The CDAO Council also serves as the principal forum to drive systemic DoD-wide strategy and policy and advocate for AI-related programmatic, institutional culture, and budgetary changes needed to facilitate the integration and fielding of AI capabilities.

The CDAO Council includes broad representation from across the Department, including but not limited to: Deputy Under Secretaries of Defense (Research and Engineering; Acquisition

and Sustainment; Policy; Comptroller; Personnel and Readiness; Intelligence and Security); Deputy Director, Cost Assessment and Program Evaluation; Principal Deputy DoD Chief Information Officer; Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency; DoD Office of General Counsel; Director of Administration and Management; Joint Chiefs of Staff Director of Operations (J3) and Director of Command, Control, Communications, and Computers / Cyber (J6); Deputy Commanders or delegated representatives of the Combatant Commands; Under Secretaries, Chief Data Officers, or other delegated representatives of the Military Departments and the National Guard Bureau.

2. Advancing Responsible AI Innovation

The Department constantly seeks to remove barriers to the responsible use of AI, such as the need for enabling infrastructure, quality data, monitoring, and testing and evaluation (T&E) resources. As the designated CAIO, CDAO advances these objectives in multiple ways.

To support the adoption and use of AI across the Department, CDAO is developing “AI scaffolding,” which will include a set of enterprise-wide capabilities, such as data labeling as a service, modeling and simulation, federated model catalogs, machine learning operations (MLOps), and test and evaluation. CDAO has also publicly released a Responsible AI (RAI) toolkit, which guides AI practitioners through tailorable and modular assessments, tools, and artifacts throughout the AI product lifecycle and enables the alignment of AI projects to RAI best practices and DoD AI Ethical Principals. CDAO has also publicly released several resources through the Joint AI Test Infrastructure Capability (JATIC) program, which develops publicly available software products for AI 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.

CDAO has evaluated the responsible fielding of generative AI (GenAI) capabilities and developed DoD-wide guidance to encourage the use of generative AI in the Department without posing undue risk. This year, CDAO issued “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. Specifically, the guidance emphasizes the following:

- Clear criteria for assessing the suitability, feasibility, and advisability of using GenAI for a particular task.
- Processes for documenting and evaluating training data quality.
- Adhering to existing cybersecurity policies and consideration of mitigations for adversarial ML attacks.
- Incorporating methods for enabling traceability and interpretability of GenAI models into GenAI tools prior to deployment.
- Assessing and mitigating undue harms, impacts, and risks.
- Following all applicable policy on sensitive information, U.S. persons data, and copyright.
- Addressing risks to effective human-machine teaming and operator trust.

CDAO has undertaken several steps to advance the Department's attraction, retention, and cultivation of AI talent. First, CDAO has an AI Talent Lead who leads the Digital Talent Management team within CDAO that oversees and executes AI talent initiatives across the Department. CDAO serves as the functional community manager for AI talent, working to provide work role coding across the Department for AI-related roles, awards for those in the DoD community who serve as positive examples of AI practitioners, and training resources for current DoD employees.

CDAO's AI Talent Lead is supporting the Department's demand for AI talent by providing foundational education and literacy pathways for data, AI, and digital transformation through the Digital on Demand platform released last year, which is available to anyone in the DoD. Our AI Talent Lead has also provided executive training for over 1,000 DoD leaders through its Leading Data and AI-Enabled Organizations series of workshops. Moreover, to attract the future AI-enabled force, CDAO has held over 125 events to reach 210,000 students.

The Department leverages hiring authorities where possible to accelerate the hiring of AI talent; the proliferation of Cyber Excepted Service (CES) roles has accelerated in recent years, and DoD Components routinely take advantage of Federal and DoD programs that place in-demand AI talent in impactful positions. Additionally, CDAO's AI Talent Lead has been establishing AI work roles across a wide range of skillsets, such as AI test and evaluation, responsible AI, AI innovation, data science, and data stewardship.

Consistent with Section 4(d) of reference (a), the Department will seek to ensure that AI code for applications in active use and data are able to be shared where practicable. While the Department is limited in its ability to share code and data publicly, it nonetheless makes ample DoD data, such as budget data, publicly available. The Defense Digital Service, now under CDAO, launched code.mil in 2017 in accordance with Office of Management and Budget Memorandum M-16-21, reference (b), to foster open collaboration with the global developer community. Code.mil provides step-by-step guidance for sharing DoD code under "How to Open Source Code." Moreover, the Department is currently pursuing a line of effort under the Responsible AI Strategy and Implementation Pathway, reference (c), which will produce further DoD guidance on the sharing or publication of DoD AI capabilities outside of the Department while preserving operational security and preventing unintended exposure.

3. Managing Risks from the Use of Artificial Intelligence

To identify use cases comprising covered AI, CDAO has incorporated the reporting of AI use cases into existing Department budget processes. For the first time, all DoD Components have been required to report their AI use cases and identify whether they meet the threshold of covered AI. To ensure the accuracy of AI use case reporting, CDAO will review all AI use case data submitted through the budget process and assess whether additional use cases meet the definition of covered AI.

In parallel, CDAO will also develop guidance for requesting waivers and implementing the minimum risk management practices outlined in reference (a), which all DoD AI practitioners will be required to follow when working on covered AI use cases. Once CDAO

identifies instances of covered AI through its updated budget process, it will work closely with each use case as needed to ensure that the minimum risk management practices are properly implemented. Component Responsible AI (RAI) Leads will be responsible for tracking determinations of covered AI within their Component and reporting their Component's compliance with the minimum risk management practices, including the termination of non-compliant covered AI. To certify compliance, all DoD Components with covered AI use cases will submit a signed memorandum to CDAO documenting their compliance with required minimum risk management practices and termination of any non-compliant covered AI.

When requesting waivers from implementing minimum risk management practices for covered AI, Components will have to provide a detailed justification and outline any risk management practices that they will implement regardless of the waiver request being granted. All waiver requests from DoD Components in the Office of the Secretary of Defense and the Fourth Estate (e.g., Defense Contract Management Agency) must be submitted to CDAO for consideration and determination. Requests for waivers for covered AI use cases within the Services will be directed to the Chief AI Officer (CAIO) designated by each Service in response to reference (a). CDAO and the Services will centrally track and evaluate waivers granted to covered AI use cases and report them to OMB as required.

The Department will continue to embrace best practices for effective AI governance and risk management while striving to attract, retain, and cultivate top AI talent. As AI capabilities become more widespread and sophisticated, the DoD will respond with agility and flexibility to advance its responsible adoption of AI.

PLUMB.RADHA.IYE
NGAR.1410463764

Digitally signed by
PLUMB.RADHA.IYENGAR.14104
63764
Date: 2024.09.19 15:45:47 -04'00'

Dr. Radha Iyengar Plumb