DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

ADS-GOV-AI-024

SAIS-ADS (25-1rrrr)

27 June 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Chief Information Officer Guidance on Generative Artificial Intelligence and Large Language Models

1. References. See Enclosure 1.

2. Purpose. Issue guidance for the development, deployment, and use of Gen AI, including Large Language Models (LLM), within the Army.

3. Background.

a. Gen AI models present unique and exciting opportunities for the Army. These models have the potential to transform mission processes by automating and executing certain tasks with unprecedented speed and efficiency. Commanders and senior leaders should encourage the use of Gen AI tools for their appropriate use cases.

b. Gen AI refers to a class of models that autonomously create new content. These powerful AI-based algorithms have the extraordinary ability to return, humanlike responses to user-created prompts, derived from the enormous sets of data upon which they were trained.

c. The output of Gen AI tools is non-deterministic and can be delivered in the form of text, images, audio, video, or other forms of unstructured data.

d. Gen AI tools have been widely adopted due to their high performance and ease of use. However, they also present unique challenges in terms of data privacy, security, and control over the generated content. Therefore, their use should be carefully evaluated and monitored.

e. Gen AI tools are fallible and can produce “hallucinations” and biased results. Hallucinations are a phenomenon whereby responses include or incorporate fabricated data that appears authentic. Therefore, these tools must be accompanied by a robust review process which may include the critical thinking skills of human expertise.

4. Applicability. Headquarters, Department of the Army, Army Commands, Army Service Component Commands, the Army National Guard/Army National Guard of the United States, and the Army Reserve.

5. Guidance.

a. Gen AI Developers/System Owners who produce a Gen AI tool should:

(1) Be subject to existing legal, cybersecurity, information, operational security, and classification policies, as well as Gen AI-specific policy (references 1a thru 1h).

(2) Ensure System Users can easily determine which systems rely on Gen AI and System Users are able to accept or reject the output of a Gen AI model.

(3) Be aware of, and seek appropriate approvals for, processing sensitive and classified information in accordance with existing software and container security policy (references 1a and 1c).

(4) Establish processes to document the source and attributes of training data, and for versioning of the training data, before developing or fine-tuning a Gen AI model.

(5) Ensure that Gen AI tools or applications operating within the DoDIN receive appropriate Authorizing Official approval, in accordance with DoDI 8500.01 (reference 1h), prior to utilizing Government data for the creation or retraining of Gen AI and LLM tools to include integration points, access to hardware, software, and interfaces to other systems. Leverage accreditation reciprocity.

(6) Conduct testing in a controlled environment to ensure Gen AI tools operate as expected. This testing should address engineering challenges introduced by the non-deterministic nature of Gen AI. These tools may require system-level guardrails to ensure that potential anomalies do not negatively impact Army missions, in accordance with the DoD Responsible AI Toolkit (reference e)

(7) Leverage existing Gen AI models when practical and consider other lower-cost mechanisms to adopt general purpose Gen AI tools to meet organizational requirements.

(8) Provide transparency and explainability for model outputs as required. This can include data lineage, documentation on model training data and specify what components are leveraging Gen AI.

b. Gen AI System Users:

(1) System Users have sole responsibility for their input and acceptance of output from Gen AI tools and should have no expectations of privacy with respect to those inputs. Misuse of government software should be treated in accordance with existing policy (references 1a and 1e).

(2) System Users are responsible for information inputted into publicly accessible Gen AI tools and are subject to existing legal, cybersecurity, information, operational security, and classification policies, as well as Gen AI-specific policy. Closed-domain tools may process information and data in accordance with their accreditation.

(3) System Users are not inherently responsible for Gen AI tool output. However, System Users are responsible for products and decisions made with the assistance of Gen AI. System Users should distrust and verify all outputs prior to use.

(4) System Users should label any document that was created—in whole or in part—with outputs from Gen AI tools. System Users should apply their best judgment when determining whether to add a citation, based on factors including the importance of transparency for a particular use case.

c. Commands Using Gen AI Tools:

(1) Commands are discouraged from banning the use of Gen AI tools. Instead, develop appropriate governance processes that holistically weigh the benefits of Gen AI tools against potential risks.

(2) Commands are responsible for identifying their Gen AI Developers, System Owners, and System Users to mitigate residual risk when adopting Gen AI tools into their workflows.

(3) Commands should ensure Developers, System Owners and Users use appropriate risk assessment frameworks for Gen AI tools. These include the DoD Responsible AI Toolkit (reference 1e), the National Institute of Science and Technology's Risk Management Framework (reference 1a), and the Defense Innovation Unit's Responsible AI Guidance (reference 1d).

(4) Commands should ensure Developers, System Owners, and Users that who utilize Gen AI tools on commercial networks (including third-party and contracted capabilities) seek Army CIO approval before utilizing Government data for the creation or retraining of Gen AI and LLM tools, to include integration points, access to hardware, software, and interfaces to other systems when operating government data. Requests for approval should be directed to the Office of the Chief Information Officer (OCIO),

Standards and Compliance Division (SAIS-ADS), via Enterprise Task Management Software Solution (ETMS2). Commands should provide the following documentation with their submission:

(a) Gen AI Tool Description: Detailed description of the AI tool, including its Developer/System Owner and System Users, purpose, capabilities, and the type of AI it uses (for example, machine learning, deep learning, etc.).

(b) Data Usage Plan: Command-approved plan outlining how government data will be used for the creation or retraining of an AI tool. This should include what data will be used, how it will be processed, and how it will be protected.

(c) Integration Details: Implementation plan outlining how the AI tool will be integrated into existing systems. This should include details about required hardware, software, and interfaces.

(d) Third-Party and Contracted Capabilities: Clearly identify and describe if utilizing third-party or contracted AI capabilities, to include dependencies on external software or services.

(e) Cybersecurity Strategy: A description of the security measures that will be put in place to protect Government data. These could include encryption methods, access controls, and audit trails.

(5) Commands should track and manage AI tools, articulate what AI tools are being developed, and how the AI tools will be utilized IAW the 5 DoD AI Ethical Principles (reference 1i).

(6) Commands should register and/or account for all existing and new AI investments whether stand-alone, embedded, or treated as applications, in the Army's Portfolio Management Solution (APMS) in accordance with AR 25-1 (reference 1j).

d. Data Stewards and Command Chief Data and Analytics Officers (C2DAO) are responsible for determining and approving the release of data for their respective functional domain or organization prior to its utilization of data outside the DODIN. (reference 1n).

6. Effective date.

a. This clarifying guidance is effective immediately and stays in effect until superseded, rescinded, or incorporated into Army regulation.

b. OCIO Standards and Compliance Division will review this guidance annually for revision by 1 October of each calendar year.

7. Points of contact.

a. CIO Policy Inbox: usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil.

b. SAIS-ADS: Dr. Gregory C. Smoots, Deputy Director, Architecture, Data, Standards at gregory.c.smoots.civ@army.mil.

GARCIGA.LEONEL.T.1186170411
Digitally signed by GARCIGA.LEONEL.T.1186170411
Date: 2024.06.27 11:14:49 -04'00'

2 Encls
1. as
2. Glossary

LEONEL T. GARCIGA
Chief Information Officer

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Futures Command
U.S. Army Pacific
U.S. Army Europe and Africa
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
U.S. Army Cyber Command
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Human Resources Command
U.S. Army Corrections Command
U.S. Army Recruiting Command
Superintendent, U.S. Military Academy
(CONT)

DISTRIBUTION: (CONT)
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency
Executive Director, Military Postal Service Agency
Director, U.S. Army Criminal Investigation Division
Director, Civilian Protection Center of Excellence
Director, U.S. Army Joint Counter-Small Unmanned Aircraft Systems Office
Superintendent, Arlington National Cemetery
Director, U.S. Army Acquisition Support Center

CF:
Principal Cyber Advisor
Director of Enterprise Management
Director, Office of Analytics Integration
Commander, Eighth Army

REFERENCES

a. NIST (Artificial Intelligence Risk Management Framework (AI RMF 1.0)), 26 January 2023. Available at https://doi.org/10.6028/NIST.AI.100-1.

b. Deputy Secretary of Defense (Implementing Responsible Artificial Intelligence in the Department of Defense), 26 May 2021.

c. DoDI 5200.48 (Controlled Unclassified Information (CUI)).

d. Defense Innovation Unit (Responsible AI Guidance) 1 May 2023.

e. DoD (Responsible Artificial Intelligence (RAI) Toolkit). Available at https://www.defense.gov/News/Releases/Release/Article/3588743/cdao-releases-responsible-ai-rai-toolkit-for-ensuring-alignment-with-rai-best-p/.

f. DoDD 5000.01 (The Defense Acquisition System).

g. DoDI 5000.82 (Requirements for the Acquisition of Digital Capabilities).

h. DoDI 8500.01 (Cybersecurity Policy).

i. Deputy Secretary of Defense memorandum (Artificial Intelligence Ethical Principles for the Department of Defense), 21 February 2020.

j. AR 25-1 (Army Information Technology).

k. GAO-23-105850 (DoD Needs Department-Wide Guidance to Inform Acquisition), 29 June 2023.

l. Deputy Secretary of Defense (DoD Data, Analytics, and Artificial Intelligence Adoption Strategy), November 2023. Available at https://www.ai.mil/references.html

m. Deputy Secretary of Defense (Responsible Artificial Intelligence Strategy and Implementation Pathway), June 2022.

n. DoD (Data Strategy), 30 September 2022

o. DA Pam 25-1-1 (Army Information Technology Implementation Instructions).

GLOSSARY

TERM	DEFINITION
Data Steward	Establish policies governing data access, use, protection, quality.
GenAI	Generic term for any AI system that generates content such as text, imagery, or other modalities.
GenAI model	An algorithm that learns the pattern and structures of training data and creates new outputs based on what it has learned.
GenAI tool	A user-facing product that is built around a GenAI model or system of GenAI models.
Use Case	A concept used in software development, product design, and other fields to describe how a system can be used to achieve specific goals or tasks. It outlines the interactions between users or actors and the system to achieve a specific outcome.