DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

NAVMC 5239.1
DC I (SDO)
4 DEC 2024

NAVMC 5239.1

From: Deputy Commandant for Information, Service Data Office
To: All HQMC Departments, Staff Agencies and Offices, All Fleet Marine Forces

Subj: UNITED STATES MARINE CORPS GUIDANCE ON GENERATIVE ARTIFICIAL INTELLIGENCE

Ref: See Enclosure (1)

1. Purpose. Issue guidance for the development, deployment, and use of Generative Artificial Intelligence (GenAI), including large language models (LLM), within the Marine Corps.

2. Background.

a. GenAI capabilities present unique and exciting opportunities for the Marine Corps. These systems have the potential to revolutionize mission processes by enhancing operational speed and efficiency, improving decision-making accuracy, reducing human involvement in redundant, tedious, and dangerous tasks, and enabling real-time adaptability to dynamic operational environments. This technological advancement can significantly boost mission effectiveness and operational readiness, providing a strategic edge in modern warfare. Commanders and senior leaders should advocate for the use of GenAI tools for their appropriate use cases.

b. Per DON Guidance on the Development and Use of GenAI (ref p), "artificial intelligence" (AI) refers to machine-based systems capable of making predictions, recommendations, or decisions that influence real or virtual environments based on human-defined objectives. These systems integrate both machine- and human-generated inputs to perceive environments, abstract these perceptions into models through automated analysis, and utilize model inference to generate options for information or actions. "Generative Artificial Intelligence" is defined under the same order as encompassing a class of AI models designed to emulate the structure and characteristics of input data to create synthetic content, including but not limited to images, videos, audio, and text. GenAI is comprised of many different categories, models, and products that independently generate new content. These advanced AI algorithms possess the remarkable ability to provide humanlike responses to user prompts, leveraging the vast datasets on which they were trained. For the purposes of this memo, GenAI includes all categories, models, and types of GenAI subject to risk identified in reference "Department of Defense (DoD) guidelines and guardrails to inform governance of Generative Artificial Intelligence", which includes Unimodal or multimodal versions of LLMs, Generative Adversarial Networks (GANs), Neural Radiance Fields (NeRFs), Transformer-Based Models, Diffusion Models and Variational autoencoders (VAEs).

c. The output of GenAI tools is often non-deterministic, meaning that the results produced by GenAI tools can vary each time you use them, even with the same input. This output can be delivered in the form of text, images, audio, video, or other forms of data that does not follow a defined format.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

d. GenAI tools present unique challenges in terms of data privacy, security, and control over the generated content. The use of such tools will be evaluated and monitored in accordance with the policies that govern the use of government information systems.

e. GenAI tools can produce inaccurate, misleading, false, and biased results. This requires an effective and continuous testing and evaluation methodology to ensure the output of GenAI models meets reasonable expectations.

f. Commands will establish an AI Task Forces/Cells consisting of various data, knowledge management, AI and digital operations subject matter experts to assess existing and in-development GenAI offerings for applicability for use in the United States Marine Corps (USMC) and will generate a list of forthcoming preferred GenAI capabilities aligned with common use cases as a reference for USMC organizations seeking to apply GenAI solutions to their mission needs and, as applicable, endorsement for Common Management Plane (CMP). Information about the AI Task Cells and its work will be captured in an upcoming memorandum.

3. Applicability. Total Force.

4. Guidance. All GenAI pilots shall be coordinated and registered with the Service Data Officer AI registry using an approved Marine Corps designated use case intake form, thereby ensuring compatibility with future Service level capabilities and to capture appropriate lessons learned and user feedback to shape enterprise solutions.

a. Developers and system owners who produce GenAI systems:

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

(2) Responsible for ensuring users can readily determine which systems rely on GenAI and that users are able to accept or reject the output of a GenAI system.

(3) Understand and obtain appropriate approvals for processing sensitive and classified information in accordance with existing software and container security policy (references a and c).

(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 GenAI model.

(5) Ensure that GenAI systems operating within the DoDIN receive appropriate authorizing official approval, in accordance with DoDI 8500.01 (reference h), prior to utilizing government data for the creation or retraining of GenAI and LLM systems to include integration points, access to hardware, software, and interfaces to other systems. Leverage accreditation reciprocity.

(6) Conduct test and evaluation in a controlled environment to ensure GenAI systems operate as expected. This test and evaluation will be conducted on a recuring basis to address engineering challenges introduced by the nondeterministic nature of GenAI. These tools may require system-level

guardrails to ensure that potential anomalies do not negatively impact missions, in accordance with the DoD Responsible AI Toolkit (reference e).

(7) Provide transparency and explainability for model outputs as required. This can include data lineage, documentation on model training data and specify what components of the overall system leverage GenAI.

b. System users that utilize GenAI capabilities are:

(1) Responsible for their input to a GenAI system and have no expectations of privacy with respect to that input.

(2) Responsible once they have accepted the output from a GenAI system. Misuse of government software is treated in accordance with existing policy (references a and e).

(3) Responsible for the information they input into publicly accessible GenAI systems and must adhere to existing legal, cybersecurity, information, operational security, and classification policies, as well as GenAI-specific policy. Closed-domain tools may process information and data in accordance with their accreditation.

(4) Responsible for products and decisions made with the assistance of GenAI. System users should distrust and verify all outputs prior to use.

(5) Responsible for labeling any document that was created, in whole or in part, with outputs from GenAI tools. Users should apply their best judgment when determining whether to add a citation, based on factors including the importance of transparency for a particular situation.

c. Commands Using GenAI Systems:

(1) Commands are discouraged from banning the use of GenAI capabilities. Instead, it is recommended to align to the enterprise service level standards and to define specific domain standards aligned to the Service. Commands should develop comprehensive governance processes that thoughtfully balance the benefits of GenAI tools and capabilities with potential risks, ensuring their use supports broader organizational objectives while maintaining operational security and integrity.

(2) Commands are responsible for identifying their GenAI developers, system owners, and system users to mitigate residual risk when adopting GenAI tools into their workflows.

(3) Commands are responsible for ensuring developers, system owners and system users use appropriate risk assessment frameworks for GenAI systems. 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 are responsible for ensuring developers, system owners, and users that utilize GenAI systems on commercial networks (including third-party and contracted capabilities) obtain an authority to operate

(5) Commands will track and manage AI tools, articulate what AI tools are being developed, and how the AI tools will be utilized in accordance with the five DoD AI Ethical Principles (reference i).

(6) Commands will register and account for all existing and new AI investments whether stand-alone, embedded, or treated as applications.

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 n).

6. Effective Date.

a. This guidance is effective immediately and stays in effect until superseded, rescinded, or incorporated into Marine Corps policy.

b. The Deputy Commandant for Information Service Data Office (SDO) will review this guidance annually by 1 October of each calendar year.

7. Points of Contact.

a. Dr. Colin Crosby, colin.crosby@usmc.mil, Service Data Officer and Deputy DON CDO

M.G. Carter

M. G. CARTER
LtGen, USMC

PCN: 10048005900

List of References

(a) DON CIO Memo, *Department of the Navy Guidance on the Use of Generative Artificial Intelligence and Large Language Models* (superseded), Sep 06, 2023

(b) EO 14110, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, Oct 30, 2023

(c) DoD Chief Data and Artificial Intelligence Officer memo, *DoD Guidelines and Guardrails to Inform Governance of Generative Artificial Intelligence*, Jul 12, 2024

(d) Joint Artificial Intelligence Center, The Department of Defense AI Ethical Principles, Feb 24, 2020

(e) Department of Defense, Responsible Artificial Intelligence Strategy and Implementation Pathway, Jun 2022

(f) Department of Defense AI Cybersecurity Risk Management Tailoring Guide, Jul 2, 2024

(g) NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), Jan, 2023

(h) NIST, 600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, Jul, 2024

(i) Department of Defense, DoDI 8500.01, Cybersecurity Program, Oct 7, 2019

(j) Department of Defense, DoDI 8510.01, Risk Management Framework for DoD Systems, Jul 19, 2022

(k) Department of Defense, DoD Responsible AI Toolkit. https://rai.tradewindai.com/

(l) DoDI 5200.48, Controlled Unclassified Information

(m) Department of Defense Data, Analytics, and Artificial Intelligence Adoption Strategy, Jun 27, 2023

(n) National Defense Strategy, Oct 27, 2022

(o) National Defense Authorization Act for FY24, Dec 14, 2023

(p) DEPSECDEF Memo, *Implementing Responsible Artificial Intelligence in the Department of Defens*e, May 26, 2021

(q) EO 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, Dec 8, 2020

(r) Office of Management and Budget M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, Mar 28, 2024

(s) NIST, Securing Large Language Model Development and Deployment, retrieved from https://www.nist.gov/system/files/documents/2024/02/01/NIST-LLMs-Nick-Hamilton.pdf , Aug 14, 2024

(t) Federal Data Strategy 2021 Action Plan, 2021

(u) National Artificial Intelligence Initiative Act of 2020, Jan 1, 2021

(v) EO 13859, *Maintaining American Leadership in Artificial Intelligence*, Feb 11, 2019

(w) Department of Defense, DoD Data Strategy: Unleashing Data to Advance the National Defense Strategy, Sep 30, 2020

(x) Joint Artificial Intelligence Center, 2020 Department of Defense Artificial Intelligence Education Strategy, Sep, 2020

(y) MCO 5231.4, *Marine Corps Data and Artificial Intelligence*, Mar 2024

(z) DEPSECDEF memo, *Creating Data Advantage*, May 5, 2021

(aa) US Marine Corps, Artificial Intelligence Strategy, Jul 8, 2024

(bb) Defense Innovation Unit, Responsible AI Guidelines. https://www.diu.mil/responsible-ai-guidelines

(cc) DEPSECDEF memo, *Establishment of the Chief Digital and Artificial Intelligence Officer*, Dec 8, 2021

(dd) DEPSECDEF memo, *Initial Operating Capability of the Chief Digital and Artificial Intelligence Officer*, Feb 1, 2022

(ee) DEPSECDEF memo, *Role Clarity for the Chief Digital and Artificial Intelligence Officer*, Feb 1, 2022

(ff) Department of Defense, DoD Strategic Management Plan for FY22-26

(gg) DoDD 3000.09, Autonomy in Weapon Systems, Jan 25, 2023

(hh) SECNAV, Department of the Navy Information Superiority Vision 2.0, Aug 16, 2024

(ii) SECNAV memo, *Department of the Navy Actions to Data Advantage*, Jun 24, 2021)

(jj) Department of the Navy, I-Plan for DoD Data Strategy (2020)

(kk) OPNAV N2N6, Navy Blueprint for a Modern Enterprise Information Ecosystem, Sep 2023

(ll) Marine Corps Chief Information Officer, Marine Corps Information Environment Enterprise Blueprint, Mar 31, 2019

(mm) U.S. Marine Corps, Force Design 2030, Annual Update, Jun 2023
(nn) U.S. Marine Corps, Data Implementation Plan, Dec 7, 2021
(oo) U.S. Marine Corps, Data Roles and Definitions, Dec 7, 2021