



# DIRECTIVE

---

**Subject: GENERATIVE ARTIFICIAL INTELLIGENCE**

<b>Number: D-431.1</b>	<b>Approved: 1/29/2026</b>	<b>Review: 1/29/2031</b>	<b>Certified:</b>
------------------------	----------------------------	--------------------------	-------------------

**Responsible Office: Division of Information Technology**

---

1. **PURPOSE.**

The purpose of this directive is to set the terms for acceptable use of generative artificial intelligence (AI) to support the Defense Nuclear Facilities Safety Board (“DNFSB” or “Board”) mission and to establish adequate safeguards and oversight mechanisms to allow generative AI tools to be used without posing undue risk.

2. **CANCELLATION.**

None.

3. **APPLICABILITY.**

This directive applies to all DNFSB personnel, including full-time employees, contractors, consultants, interns, and any individuals granted access to DNFSB systems, data, or networks. It governs the use of all generative and analytical AI tools—whether public, commercial, or internally developed—used in support of DNFSB mission activities.

4. **EXEMPTIONS.**

None.

5. **OPERATIONAL DIRECTION.**

In accordance with Administration policy<sup>1</sup>, the DNFSB will employ American generative AI technology to support mission delivery and promote operational efficiency. A governance and risk management framework will ensure responsible use of mission-enabling AI tools and safeguard sensitive data. Risk management protocols will use a graded approach where use cases<sup>2</sup> with higher potential adverse impacts will be managed with more stringent oversight and controls. To deploy AI tools in a manner that

---

<sup>1</sup> Executive Order (EO) 14179, *Removing Barriers to American Leadership in Artificial Intelligence*.

preserves public trust, the DNFSB will always ensure agency decisions and final work products are prepared and reviewed by qualified experts and responsible managers. While AI technology is an increasingly powerful mission-enabling tool, generative AI will not serve as a substitute for human judgment and all employees remain ultimately responsible for the content and accuracy of their work.

6. **REQUIREMENTS.**

A. Governance and Oversight

- i. The Executive Director of Operations (EDO) will designate a Chief AI Officer and the members of the AI Council to coordinate all DNFSB activities related to acquisition, development, deployment, use, and management of generative AI systems and tools. The Chief AI Officer will lead the agency's AI Council, update and maintain the DNFSB's AI use case inventory and advise agency leadership on all AI-related matters. The Chief AI Officer will also represent the DNFSB in interagency bodies and communities of practice formed to advance the responsible use of generative AI across the federal government.
- ii. The AI Council, established as a standing committee, will evaluate new AI use cases prior to implementation. The AI Council will include multi-disciplinary expertise (e.g., legal, cybersecurity, and end user representatives) drawn from across the agency. The AI Council will determine whether proposed AI applications meet defined criteria<sup>3</sup> for high impact use cases and prepare documentation to update the agency's AI use case inventory. The AI Council will provide a recommendation to the EDO, or designee, who will serve as the approval authority for new AI use cases.
- iii. To manage risk and ensure transparency, the DNFSB will maintain an inventory of approved AI use cases. Whenever the EDO, or designee, approves a new AI use case, the Chief AI Officer will update the inventory using information prepared by the AI Council. In accordance with Office of Management Budget (OMB) requirements, the AI use case inventory will be posted to the DNFSB's public website (excluding any controlled unclassified information) and this external posting will be updated at least annually.

---

<sup>3</sup> The AI Council will use 'high impact' determination criteria defined in OMB Memorandum M-25-21, *Accelerating Federal Use of AI through Innovation, Governance and Public Trust*.

B. Acceptable Use of Generative AI

i. General Rules of Behavior

- (1) Generative AI tools accessed through DNFSB information technology systems are intended for mission-enabling purposes.
- (2) Users are responsible for verifying the accuracy of information obtained from generative AI systems. The level of effort applied to verify the accuracy of information output by generative AI should be commensurate with the importance of its intended application. When using citations that are listed in generative AI outputs, users must consult the cited source material to confirm that information has been quoted or interpreted accurately.
- (3) Generative AI outputs will not be used directly (i.e., without human intermediation) in agency decisions or work products. Output from generative AI will always be independently evaluated and subjected to expert review for accuracy by qualified agency personnel before informing any DNFSB activity. Generative AI will not serve as the sole or primary basis for agency action or output.
- (4) Classified information will never be used in any AI application accessed through the DNFSB information technology system.
- (5) Federal non-public information, including Controlled Unclassified Information (CUI) (e.g., Personally Identifiable Information, Privacy Information, Legal Privilege Information, and Unclassified Controlled Nuclear Information (UCNI)) may only be used within approved secure enterprise systems.
- (6) User inputs to public generative AI systems must avoid disclosing sensitive or non-public information.
- (7) When using generative AI systems on agency information technology networks, users must report to the Chief AI Officer any significant issues or anomalies that raise safety, security, privacy, or operational concerns.

ii. Use Case Categories

- (1) AI use cases at the DNFSB are categorized as follows:
  - (a) Capability Assessment: Explore and assess AI tools using only non-sensitive and publicly available information.
  - (b) Pre-Deployment: Performance of limited and controlled research and development testing to assess utility and optimize safeguards for AI use cases proposed for eventual widespread agency deployment.

- (c) Pilot: Trial implementation of an AI use case within a defined user base of beta-testers. Pilots may be used to test complex or potentially sensitive AI use cases prior to initiating full-scale deployment.
- (d) Deployed: An AI use case implemented through an approved AI system and available to agency users.
- (e) Retired: An AI use case that was previously in a pre-deployment, pilot, or deployed status, but is no longer in active use.

iii. Approval Process for New AI Use Cases

- (1) To propose a new AI use case for evaluation, any agency employee may contact the AI Council ([AIUseCase@dnfsb.gov](mailto:AIUseCase@dnfsb.gov)) to submit the following information:
  - (a) Purpose statement and general description of the AI use case.
  - (b) Data sets needed to implement the AI use case and an indication of whether any required data includes sensitive or non-public information.
    - (i) If a use case involves sensitive or non-public data, specify the approved AI system(s) that will implement the use case.
  - (c) The problem the AI use case intends to solve and its expected benefits.
  - (d) Expected outputs of the AI use case.
- (2) The AI Council will perform the following functions in evaluating proposals for new AI use cases:
  - (a) Document a determination of whether the proposed use case meets the high impact criteria defined in OMB Memorandum M-25-21.
    - (i) If an AI use case is determined to meet high impact criteria, this application cannot be implemented until the DNFSB establishes minimum risk management practices and internal controls for high impact use cases.
  - (b) Perform a risk assessment of the proposed AI use case to identify potential harms that could arise from implementation and prescribe controls to prevent or

mitigate harms. Risk assessments should address at least the following potential harms and candidate controls:

- (i) Potential harms
  - 1. Issues that could impact public trust.
  - 2. Issues that could compromise or corrupt agency data or information technology systems.
  - 3. Issues that could lead to the unauthorized disclosure of sensitive or non-public data.
  - 4. Issues that could result in classified information being inadvertently generated and stored on unauthorized systems.
  - 5. Any other significant risk that could harm agency standing or operations.
- (ii) Potential controls
  - 1. Technical measures implemented through the agency information technology system, including automated monitoring and use controls.
  - 2. Administrative measures, including requirements and guidance, embedded within agency policies and procedures.
  - 3. Training to reinforce and strengthen the reliability of technical and/or administrative controls.
  - 4. Any other control necessary to prevent or mitigate significant potential harms from an AI use case.
- (c) Describe the general path for the AI use case to transition from initial approval to deployed status, including expectations for piloting or controlled testing and evaluation.
- (d) Define the user base for the AI use case upon full deployment and specify any necessary access controls.
- (e) Prepare and deliver a recommendation to the EDO, or designee, that summarizes the results of the high impact determination, risk assessment, deployment road map, and access controls.

- (3) The EDO, or designee, will review the recommendation of the AI Council on a proposed use case and either approve, disapprove, or request additional information.
  - (a) The EDO, or designee, may conditionally approve a new use case and require additional review and approval prior to full deployment of the application.
- (4) Upon approval by the EDO, or designee, the Chief AI Officer will update the agency use case inventory and coordinate implementation of the newly approved AI use case and any associated controls.

iv. Existing Use Cases

- (1) The Chief AI Officer will monitor implementation of existing use cases and associated controls.
  - (a) The Chief AI Officer will convene the AI Council, as necessary, to discuss any new information that could alter the understanding of either risks or controls for an existing AI use case.
- (2) The Chief AI Officer will determine when an existing approved AI use case is ready to transition to a new phase of implementation (e.g., pilot, deployed, retired) and will update the agency use case inventory, as necessary.

C. Cybersecurity

- i. All AI systems and use cases at the DNFSB must adhere to strict cybersecurity and technical requirements to protect sensitive data, maintain system integrity, and safeguard public trust.
- ii. All approved AI systems and use cases must be integrated into DNFSB's Zero Trust Architecture, ensuring continuous verification of users, devices, and access privileges, with no implicit trust within the network.
- iii. All approved AI systems and use cases must use American AI technology and models.
- iv. User inputs and outputs containing CUI must be encrypted at rest and in transit within approved AI systems.
- v. In coordination with the Chief AI Officer, the DNFSB IT and cybersecurity teams must conduct regular vulnerability assessments to ensure high availability, fault tolerance, and compliance with applicable federal standards.

## DNFSB D-431.1 Generative Artificial Intelligence

### D. Data Protection

- i. Any AI system that processes federal non-public information (including CUI or UCNI) must satisfy the following requirements:
  - (1) Operate in accordance with an approved System Security Plan.
  - (2) For cloud-hosted AI systems, demonstrate Federal Risk and Authorization Management Program (FedRAMP)/Federal Information Security Modernization Act (FISMA) authorization to operate at a Moderate impact level, or higher.
  - (3) Furnish information about the use of external application programming interfaces (API) or third-party AI services, such as those provided by commercial AI vendors (e.g., OpenAI, Google)
  - (4) Prohibit the retention or use of non-public inputted agency data and outputted results to further train publicly or commercially available AI models.

### E. Monitoring and Auditability

- i. Use of generative AI on the DNFSB information technology system will be continuously monitored, with input and output activity logged, timestamped, and securely stored to enable auditability and incident response.

### F. Incident Response

- i. Any adverse issues or anomalies involving AI systems accessed through the DNFSB information technology system must be reported to the Chief AI Officer immediately.
- ii. The Chief AI Officer will document AI-related incidents in the DNFSB Cybersecurity Incident Response Log and coordinate an appropriate response.
- iii. Based on lessons learned from significant incidents, the Chief AI Officer will initiate updates to any affected use case risk assessments to ensure controls for AI use cases remain adequate.

### G. Minimum Requirements for High Impact AI Use Cases

- i. The DNFSB will establish requirements and internal controls to manage the increased risks inherent in the use of AI tools for high impact AI use cases prior to the authorization of such use cases.

7. **RESPONSIBILITIES.**

A. Executive Director of Operations

- i. Sets agency direction on the adoption, governance, and responsible use of AI technology to enhance mission delivery and operational efficiency.
- ii. Ensures implementation of AI technology supports agency interests and aligns with Administration priorities.
- iii. Designates the agency's Chief AI Officer and members of the AI Council.
- iv. Provides executive direction to the AI Council on scope and objectives.
- v. Serves as the approval authority (unless delegated) for:
  - (1) Acquisition and utilization of secure AI systems for agency use.
  - (2) New AI use cases that require reporting in accordance with OMB Memorandum M-25-21.

B. Chief AI Officer

- i. Promotes agency-wide responsible AI innovation and adoption in accordance with appropriate governance and risk management processes.
- ii. Coordinates with other responsible officials to ensure that DNFSB use of AI complies with applicable law and Administration guidance.
- iii. Serves as the senior advisor on AI to agency leadership and within DNFSB's executive decision-making bodies.
- iv. Chairs the AI Council and coordinates its critical functions.
- v. Maintains and updates the agency's AI use case inventory and ensures a current version of the inventory is posted to the DNFSB's public website at least annually.
- vi. Determines when approved AI use cases may transition from one implementation category to another (e.g., transition from pre-deployment to pilot).
- vii. Coordinates agency review and approval of secure AI systems to ensure these systems meet all applicable cybersecurity and data protection requirements.
- viii. Represents the DNFSB in interagency bodies and communities of practice dedicated to advancing the responsible use of AI across the federal government.

C. AI Council

- i. Serves as the DNFSB's multi-disciplinary body to evaluate AI-related issues and makes recommendations to agency leadership.

## DNFSB D-431.1 Generative Artificial Intelligence

- ii. Formulates and updates agency policies and requirements governing responsible use of AI technology.
- iii. Documents high impact determinations and performs risk assessments for proposed AI use cases.

### D. General Counsel

- i. Designates a legal representative as a member of the AI Council to advise the AI Council on legal and regulatory compliance of AI use cases.

### E. DNFSB Personnel

- i. DNFSB personnel are responsible for the quality and accuracy of their work products regardless of whether the work product was created in part or completely through the use of an AI tool.
- ii. Leverage the use of AI tools to improve the efficiency and effectiveness of work processes.
- iii. Use AI tools consistent with approved use cases and subject to applicable requirements for information security.

## 8. **CONTROLS AND MEASURES.**

- A. The Chief AI Officer will periodically conduct and document assessments of agency implementation of requirements and processes governing generative AI use to ensure risks are being appropriately managed and to identify any barriers inhibiting effective use of AI technology in support of the DNFSB mission.

## 9. **REFERENCES.**

- A. Executive Order 14179, *Removing Barriers to American Leadership in AI.*
- B. Office of Management and Budget Memorandum M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust.*
- C. Office of Management and Budget Memorandum M-25-22, *Driving Efficient Acquisition of AI.*
- D. D-22.1, *Internal Control Program.*
- E. D-401.1, *Acceptable Use of Information Technology Resources.*

10. **DEFINITIONS.**

- A. **Artificial Intelligence.** A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis in an automated manner, and use model inference to formulate options for information or action.
- B. **Artificial Intelligence System.** Any data system, software, hardware, application, tool, or utility that operates in whole or in part using dynamic or static machine learning algorithm or other forms of AI; but does not include any common commercial product within which AI is embedded, such as a word processor or map navigation system.
- C. **Generative Artificial Intelligence.** The class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content. This can include text, images, video, audio, and other digital content.
- D. **Use Case.** A systematic application of AI technology to address specific challenges or improve existing processes within the agency.

11. **APPROVAL.** The General Counsel has concurred on this Directive.

12. **CONTACT.** Address questions concerning this Directive to the Chief AI Officer.

---

Mary Buhler  
Executive Director of Operations