U.S. DEPARTMENT of ENERGY

U.S. Department of Energy

Artificial Intelligence Compliance Plan

October 2025

Table of Contents

Introduction

This document was prepared by the Chief Artificial Intelligence Officer (CAIO), the Office of Critical and Emerging Technologies (CET), and the Office of the Chief Information Officer (OCIO) of the Department of Energy.

Driving Artificial Intelligence (AI) Innovation

Removing Barriers to the Responsible Use of AI

- The Department of Energy (DOE) is challenged with providing tools and maintaining compliance with evolving cybersecurity standards in the wake of evolving threat vectors. Staff are unable to access and utilize the advanced AI tools and services provided by leading cloud service providers (CSPs) as many critical services are awaiting FedRAMP authorization necessary to protect the public interest, including protecting confidential[1] and protected[2] information from unauthorized or inadvertent disclosure. Furthermore, there are feature parity gaps between the commercial offerings and the Federal government-specific cloud environments. While this feature gap is closing, it is likely that the gap will continue as CSPs roll out new services and capabilities. Furthering the challenge is that existing cloud management security practices elongate the timeline between a service achieving FedRAMP approval and when the Department can offer those services to developers within the context of the existing managed cloud environments. The IT infrastructure barrier extends beyond the serverless CSP services to the availability and timeliness of securing virtual machines with the requisite Graphics Processing Unit (GPU) hardware to develop, train, manage, and deploy advanced AI models. This challenge is industry-wide; however, it will impact the rollout and adoption of more advanced customized use cases that require dedicated GPU hardware.

Sharing and Reuse

- The existing data infrastructure lacks the necessary integration, governance, and management capabilities to support AI adoption effectively. This is evidenced through fragmented data sources, inconsistent data quality, and inconsistent and insufficient data interoperability standards. DOE recently published its Enterprise Data Strategy and Open Data Plan, which outline the steps the Department is taking to improve its data sharing and reuse.

- DOE's Office of Scientific and Technical Information (OSTI) fulfills agency-wide responsibilities to collect, preserve, and disseminate both unclassified and

---

[1] 18 U.S.C. § 1905.
[2] Authorities protecting certain data from public dissemination include 15 U.S.C. § 3710a(c)(7) (cooperative research and development agreements), 42 U.S.C. § 13541(d) (Energy Policy Act of 1992), 15 U.S.C. § 638(j)(2)(A), (p)(2)(v) (small business grant programs), and 42 U.S.C. 7256(g)(5) (other transactions).

classified scientific and technical information (STI) emanating from DOE-funded research and development activities. To serve this mission, OSTI publicly hosts unclassified DOE R&D results at OSTI.GOV and provides application programming interfaces to support AI and large-scale analysis use cases. Specifically for scientific software, OSTI developed DOE CODE, a public software services platform and search tool for software and code resulting from DOE-funded research that provides functionality for collaboration, archiving, and discovery of scientific and business software funded by DOE. This platform serves as a mechanism for sharing AI and other scientific code with the public, as all DOE National Laboratories, facilities, and contractors are required to announce their software using DOE CODE.

- Additionally, DOE's Office of Technology Commercialization (OTC) launched the Visual Intellectual Property Search database, known as VIPS, in July 2024 to make it easier for the public to perform intellectual property (IP) searches and find new technologies developed at DOE's 17 National Laboratories and several additional DOE plants and sites. Within this database, members of the public and other Federal agencies can search for AI and machine learning IP generated by DOE. Entries include open-source code that can be used to access models and AI assets.

- DOE promotes code sharing, models, and other AI assets internally through several AI working groups, including the Headquarters and National Lab Subgroup, AI Community of Interest, and AI Community of Practice.

- DOE's Office of Scientific and Technical Information (OSTI) in consultation with Program Offices and the Office of General Counsel ensures that data is released without any unintended disclosure.

- DOE's Office of the General Counsel is consulted if models require training on data that has any protective markings.

AI Talent

- DOE has been at the forefront of advancements in technology and science since its inception. For decades, our scientists, engineers, and technologists have been advancing developments in AI, and the Department is committed to transforming, attracting, retaining, and training a workforce that will help promote the United States' leading the world in AI innovation. To transform the current workforce and develop the next generation of AI talent, DOE, and the National Science Foundation (NSF) have launched a pilot program to train 500 new

researchers by 2025 to meet the rising demand for AI talent. Addressing both the needs of the current workforce and the development of emerging AI professionals.

- To ensure effective coordination, the Office of Human Capital (HC) was designated as the Agency AI Talent Lead for DOE and is responsible for working across the Department to align AI positions toward a common goal. HC has several existing and planned initiatives aimed at increasing the Department's AI talent and capacity.
- DOE completed the government-wide AI Talent and AI Enabling Talent Data Call and began completing its internal workforce planning using this exercise to identify and track its Federal AI positions and vacancies. HC plans to update position descriptions to reflect those additional job responsibilities. Once complete, HC will assign AI work roles from the Department of War Cyber Workforce Framework to better identify the skillsets associated with those positions.

Improving AI Governance

AI Governance Board

- The U.S. Department of Energy Artificial Intelligence (AI) Governance Board (AIGB) (Board) is the principal forum for improving collaboration and coordination of broad AI-related activities across the DOE enterprise. The Board is the mechanism that DOE uses to govern AI issues across the Department, focusing on AI for DOE operations as well as developing a broader strategy for AI to advance the Department's mission.
- **The AIGB will:**
    - Develop governance for DOE's research, development, deployment, and utilization of AI technologies and tools, including to remove barriers to the Departmental use of AI and to manage high-impact use cases and protect confidential and protected information from unintended disclosure.
    - Provide input on the generation and implementation of the Department's AI Strategy and any other governing documents required by OMB and the administration.
    - Empower trained and accountable agency officials at the lowest appropriate level to identify, assess, mitigate, and accept risk for AI use cases.
    - Address and coordinate on significant AI policy issues and provide recommendations that require input from multiple perspectives.

  - Contribute to DOE efforts to develop goals, priorities, and metrics for guiding and evaluating activities on AI, consistent with law, current guidance issued by the Office of Management and Budget (OMB), and other administration directives.
  - Provide recommendations to a coordinated, cross-Department annual budget request for AI initiatives, encompassing all AI research, development, and deployment activities.
  - Advise DOE senior leadership on opportunities for AI innovations to move to demonstrations and applications in support of DOE missions.
  - Discuss and implement approaches to workforce training to recruit, train and retain AI talent at the Department and within the broader DOE complex.
  - Support the annual update of the Department AI Use Case Inventory.
  - Promote the formation of industry accreditation organizations to develop Nuclear Quality standards for AI.

- **Membership**
  - The AIGB is chaired by the Deputy Secretary, vice-chaired by the Chief AI Officer (CAIO).
  - Membership of the AIGB includes representation from key stakeholder offices or components, including those responsible for addressing IT, cybersecurity, data, budget, statistics, legal counsel, privacy, civil rights, and civil liberties.(All members of the AIGB must be federal employees.)
  - The Chair and Vice-chair may request broader participation from non-governmental entities such as national labs and contractors, depending upon the topic or activity, for the purpose of receiving information from such stakeholders or when those stakeholders are presenting their individual advice and recommendations to DOE. To avoid any appearance that non-governmental entities are fixed members of the AI Governance Board, or that the AI Governance Board is giving preferential treatment to any individual or group, the AI Governance Board must avoid the regular and systematic participation of the same external stakeholders in AI Governance Board meetings. These engagements are limited to the provision of individual advice and recommendations; non-governmental stakeholders may not participate in the group decision-making process.

- **Governance**
    - The Board provides oversight and strategic direction to DOE's AI-related sub-groups, including the AI Working Group, a program-level mechanism with subject matter expert participation for cross-DOE coordination and strategy development on AI issues. The composition of the AI Working Group will include DOE elements responsible for implementing AI within DOE's program offices and other designees of the AIGB. Additional sub-groups may make recommendations to the Board within assigned areas of responsibility and escalate issues when required. The Board will resolve policy conflicts elevated by the sub-groups.

- **Frequency of Meetings**
    - The Board will meet at least annually, or more frequently as requested by the Chair and Vice-chair.

- **Operations**
    - The Director of the Office of Critical and Emerging Technologies serves as the Secretariat for the Board. With guidance from the Chair and Vice-chair, the Secretariat is responsible for ensuring that issues brought before the Board are properly analyzed and prepared for decision, that Board decisions are documented and communicated across the Board membership, and as appropriate, the DOE enterprise and stakeholders. The Secretariat will document Board decisions in a Summary of Conclusions.
    - The Board, in coordination with the Chair and Vice-chair, may seek advice from senior representatives from other elements of the U.S. Government and from experts outside the U.S. Government, in a manner consistent with applicable law.

Agency Policies

- DOE developed and published the GenAI Reference Guide in 2024 to provide an overview of the key benefits, considerations, risks, and best practices associated with the responsible development, implementation, and use of GenAI technology. This guide is focused on helping stakeholders across the DOE enterprise understand the principles for using GenAI technology responsibly, the legal framework and obligations for responsible use, and key considerations for mitigating risks. It provides guidelines for safeguards and oversight mechanisms, including keeping a human in the loop throughout the AI lifecycle, developing

review processes, and ensuring foundational security. DOE plans to update the Generative AI reference guide to a V3 to reflect recent Federal guidance.

- DOE plans to update its procurement guidance to align with OMB Memo M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government." This memo requires agencies to update internal acquisition procedures to foster a competitive U.S. AI marketplace, manage risks, and ensure cross-functional engagement in AI procurement. DOE's updated guidance will incorporate requirements for identifying high-impact AI use cases, protecting intellectual property and government data, and maximizing the use of U.S.-produced AI products and services.
- DOE plans to develop its generative AI (GenAI) policy in accordance with OMB Memo M-25-21, "Accelerating Federal Use of AI through Innovation, Governance, and Public Trust." Key aspects of DOE's policy will include guidelines for responsible use, risk assessments, and measures to protect sensitive data to mitigate potential risks while leveraging GenAI's benefits.
- DOE plans to work with the appropriate AI risk management groups across the enterprise to develop a standardized procedure in analyzing AI tools for eventual agency usage.
- DOE will continue to take steps to incorporate principles from the National Institute of Standards and Technology (NIST) AI 600-1, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile and the NIST AI RMF Playbook.

AI Use Case Inventory

- DOE has prepared and reported annual AI use case inventories since 2021 and has proven processes and tools in place to ensure information is comprehensive, complete, and adheres to OMB guidance.
- DOE will follow existing OCIO processes and procedures to conduct the annual inventory of AI use cases. A key component of DOE’s approach is leveraging a Data Call Application (DCA) capability for IT-related data calls. Using DCA enables reporting entities to easily update, add, remove, or carryover inventories from previous AI use case data collections. DCA also provides quality control mechanisms, including error checking. The DCA tool also includes an approval hierarchy that increases complete and accurate reporting.
- All Departmental Elements (DEs) and components are tasked to respond to the annual AI use case data call. OCIO develops and proactively communicates the data call schedule and requirements to all DOE stakeholders to ensure timely

and accurate inputs. In addition, the OCIO team hosts informational webinars at the onset of the data call period and holds biweekly office hours sessions to provide continuous data call and DCA support. Once the DEs have completed and approved their inventories, personnel in OCIO, in coordination with CET, will conduct a comprehensive verification and validation review prior to submitting to OMB. DOE also established an AI Use Case Inventory Working Group to aid in a consistent approach to the inventory process. The working group brings together AI leadership across DEs to share lessons learned and review new guidance.

Fostering Public Trust in Federal Use of AI

Determination of Presumed High-Impact AI

- To ensure compliance with OMB guidance, DOE created the High-Impact AI Working Group. This group represents AI equities from across the Department and will support efforts to identify high impact AI use cases. The group has developed a checklist to guide the Department in determining if an AI use case is high-impact. This checklist will be shared with all Departmental Elements for immediate use as AI efforts are planned.
- In accordance with the Federal Information Technology Acquisition Reform Act (FITARA) requirements, the OCIO reviews and approves IT acquisition strategies. As part of that review process, OCIO will request completion of the checklist for AI acquisitions to identify those that may be high-impact.
- During the annual AI use case inventory process, DEs will be asked to identify and report high-impact use cases. DOE will be developing additional processes to address AI use cases that may arise outside of the annual reporting cycle.

Implementation of Risk Management Practices and Termination of Non-Compliant AI

- DOE's High-Impact AI Working Group will provide recommendations on the implementation of risk management practices. Based on self-reporting, DOE will work with the use case owner to determine if a use case meets criteria as high impacting and confirm that the minimum risk management practices are implemented. If the use case owner is unable to implement the risk management practices, then the CAIO will determine if a waiver is appropriate, or if use case termination may be required.
- The DOE High-Impact AI Working Group will facilitate the implementation of minimum risk management practices. DOE will evaluate use cases collected during the annual AI use case inventory data call and use cases self-reported throughout the year to determine which use cases meet criteria as high-impact and confirm that the minimum risk management practices are implemented.