DEPARTMENT OF ENERGY AI COMPLIANCE PLANS PER OMB M-24-10, ON ADVANCING GOVERNANCE, INNOVATION, AND RISK MANAGEMENT FOR AGENCY USE OF ARTIFICIAL INTELLIGENCE

Prepared by Helena Fu, Acting Chief Artificial Intelligence (AI) Officer (CAIO), and Bridget Carper, Responsible AI Official (RAIO) of the Department of Energy.

1. STRENGTHENING AI GOVERNANCE

General

The Office of Critical and Emerging Technologies (CET) and the Office of the Chief Information Officer (OCIO) have undertaken efforts to update the Department of Energy's (DOE's) internal AI-related guidelines and policies consistent with the Office of Management and Budget (OMB) Memorandum M-24-10. The following efforts are planned or in place today:

Designation of an Acting Chief AI Officer (CAIO) and Responsible AI Official (RAIO)

- DOE has designated an Acting CAIO consistent with mandated policies by M-24-10. Helena Fu serves as Director of DOE's Office of Critical and Emerging Technologies (CET) and is also the Department's Acting CAIO. As the Acting CAIO, Helena is the senior advisor on AI to Departmental leadership and is responsible for coordination, innovation, and risk management in DOE's development and deployment of AI.
- DOE has designated a RAIO who is charged with deploying responsible AI practices and guidelines at DOE. Bridget Carper serves as DOE's Deputy Chief Information Officer for Architecture, Engineering, Technology, and Innovation and is also the Department's RAIO. As the RAIO, Bridget maps AI activities through a risk management program and collaborates with officials to establish processes that evaluate the performance of AI systems, ensuring DOE's compliance through the AI Hub.

Convening AI Agency Governance Bodies

- The AI Advancement Council (AIAC) is the principal forum for collaboration and coordination of AI-related activities. The AIAC provides oversight and strategic direction for DOE's use of AI.
- The Rights- and Safety-Impacting AI Working Group was stood up to support the development of new DOE internal guidelines for reviewing rights- and safety-impacting AI use cases.
- The AI and Cybersecurity Working Group is dedicated to reviewing potential cybersecurity threats of AI, understanding where AI can support new cybersecurity applications, and developing cybersecurity and AI guidance.

AI Use Case Inventories & Reporting

- Consistent with M-24-10, DOE will be conducting an annual inventory of AI use cases across the Department's program offices, 17 National Labs, Power Marketing Administrations, and field sites. To support the preparation of this data call, an AI Use

Case Inventory Working Group convenes AI leadership across DOE. Group activities include reviewing OMB guidance and past use case inventories.

- A new component of the AI Use Case Inventory includes reporting on human rights- and safety-impacting use cases. DOE's Rights- and Safety-Impacting AI Working Group is developing guidelines for evaluating human rights- and safety- impacting use cases.

Development of AI Guidelines & Policies

- DOE published Version 2 of the Generative AI (GenAI) Reference Guide in June 2024. The guide provides an overview of the key benefits, considerations, risks, and best practices associated with the responsible development, implementation, and use of GenAI technology. Constructed by over 30 DOE offices, sites, and labs, the DOE GenAI Reference Guide Version 2 reflects the latest guidance, including the October 2023 Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial
- Intelligence (EO 14110) and OMB M-24-10 guidance. This guide is focused on helping DOE stakeholders understand responsible use of GenAI technology, the legal framework and obligations for responsible use, and key considerations for mitigating risk. DOE will continue to revise and refresh the guide as needed.
- DOE will be taking steps to incorporate principles from the recently released 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.
- DOE will be conducting discovery on the agency's AI Risks and promoting collaboration on mitigating risks. In addition, we will be leveraging the CAIO Council's Risk Management Working Group for common experiences and recommended responses.
- DOE plans to update the 2022 version of its Artificial Intelligence and Risk Management Playbook (AI RMP), which is closely aligned with the NIST Risk Management Framework (RMF) and tailored to addressing AI issues relevant to DOEs mission space.
- DOE will be developing an AI policy to communicate requirements for ethical AI use, transparency in AI deployment, and risk management. This policy will align to requirements outlined in M-24-10.

AI Governance Bodies

DOE AI Advancement Council (AIAC)

The DOE AIAC is the principal forum for improving collaboration and coordination of broad AI-related activities (i) across the DOE enterprise and (ii) with external stakeholders. The AIAC provides oversight and strategic direction to DOE's AI-related sub-groups, such as the AI Working Group—a program-level mechanism with subject matter expert participation for cross-DOE coordination and strategy development on AI issues. Sub-groups may make recommendations to the Council within assigned areas of responsibility and escalate issues when required. The Council will resolve policy conflicts elevated by the sub-groups.

The Council will:

- Develop governance for DOE's research, development, deployment, and utilization of AI technologies and tools, including methods for removing barriers to the Department's use of AI and for managing its associated risks.
- Provide guidance on the current and future state of strategic AI directions to advance the Department's missions.
- Facilitate information sharing, planning, coordination, and communication of AI activities across the Department and to external stakeholders.
- 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 the requirements of the National AI Initiative Act of 2020 and EO 14110.
- Provide recommendations to a coordinated, cross-Department annual budget request for AI initiatives, encompassing all AI research, development, and deployment activities.
- Identify and define priority areas of AI research and development.
- Advise DOE senior leadership on opportunities for AI innovations to move to demonstration 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.
- Coordinate on AI partnerships with stakeholder groups—including academia and industry—that enhance national, local, and Tribal partnerships and foster long-term economic growth and job creation for DOE's AI investments.
- Identify opportunities to improve the quality and availability of standardized, secure, aggregate, and privacy-protected datasets for AI activities.

AIAC Membership

The Council is chaired by the Deputy Secretary, vice-chaired by DOE's Acting CAIO, and includes the following members, as directed by OMB M-24-10. (Note: All members of the Council must be federal employees.)

- Deputy Secretary (Chair)
- Chief Artificial Intelligence Officer (Vice-chair)
- Chief of Staff to the Secretary
- Under Secretary for Infrastructure
- Under Secretary for Science and Innovation
- Under Secretary for Nuclear Security and Administrator of the National Nuclear Security Administration (NNSA)
- Director, Office of Critical and Emerging Technologies
- Responsible AI Official
- Assistant Secretary for Electricity
- Assistant Secretary for Energy Efficiency and Renewable Energy
- Assistant Secretary for Fossil Energy and Carbon Management
- Assistant Secretary for Nuclear Energy
- Assistant Secretary for Environmental Management
- Director, Indian Energy Policy and Programs
- Director, Office of Management

- Director, Office of Legacy Management
- Director, Advanced Research Projects Agency – Energy
- Chief Information Officer (CIO)
- Associate Administrator for Information Management and Chief Information Officer (NA)
- Director, Office of Advanced Simulation and Computing & Institutional Research and Development (NA)
- Director, Office of Intelligence and Counterintelligence
- General Counsel
- Director, Office of Enterprise Assessments
- Chief Financial Officer
- Power Marketing Administration Administrators
- Director for Environment, Health, Safety, and Security, to include representation for the Senior Agency Official for Insider Threat
- Director, Office of Cybersecurity, Energy Security, and Emergency Response
- Director, Office of Science
- Director, Office of Advanced Scientific Computing Research (SC)
- Director, Office of Technology Transitions
- Director, Office of Policy
- Chief Human Capital Officer
- Director, Office of Project Management
- Director, Office of Energy Justice and Equity
- Director, Office of Small and Disadvantaged Business Utilization
- Assistant Secretary for Congressional and Intergovernmental Affairs
- Secretary of Energy (Ex Officio)

The following will participate in Council activities as needed:

- Senior Advisors in the Office of the Secretary
- Assistant Secretary for International Affairs
- Senior Procurement Executive
- Administrator of the Energy Information Administration
- Principal Assistant Deputy Administrator for Research, Development, Test, and Evaluation (NNSA)
- Inspector General
- Power Marketing Administration Chief Information Officers

AIAC Governance

The Council provides oversight and strategic direction to DOE's AI-related sub-groups, such as the AI Working Group—a program-level mechanism with subject matter expert participation for cross-DOE coordination and strategy development on AI issues. Sub-groups may make recommendations to the Council within assigned areas of responsibility and escalate issues when required. The Council will resolve policy conflicts elevated by the sub-groups.

External Engagement

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 AIAC, or that the AIAC is giving preferential treatment to any individual or group, the AIAC must avoid the regular and systematic participation of the same external stakeholders in AIAC 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.

Other routes for engagement with external experts include the Secretary of Energy Advisory Board (SEAB) and the AI Working Group. The SEAB is composed primarily of members of academia, industry, and non-governmental organizations. The SEAB provides advice and recommendations to the Secretary of Energy on the Administration's energy policies, the Department's basic and applied research and development activities, economic and national security policy, and on any other activities and operations of DOE, as the Secretary may direct. The duties of the Board are solely advisory. The Secretary has directed the SEAB to assess the Department’s role in AI development and deployment, as well as the growing energy demands of AI technologies. The AI Working Group is a working-level group composed of individuals across the DOE complex and the 17 National Laboratories dedicated to execution of EO 14110 as well as general AI development, deployment, and governance issues within the Department.

AI Use Case Inventories

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.

Reporting on AI Use Cases Not Subject to Inventory

DOE will collect AI use cases throughout the Department based on OMB final instructions. During the validation and verification phase, DOE will determine if any use cases a meet the criteria for exclusion based on M-24-10 guidance. DOE will maintain a comprehensive AI use case inventory and report externally only those use cases that meet reporting criteria in M-24-10.

DOE will validate previously reported use cases on an annual basis. DOE sites will review and verify previously reported use cases and will be prompted to reconfirm each use case's status as reportable or non-reportable. Any use case that no longer meets the criteria of non-reportable will be reclassified and included in the DOE use case inventory as appropriate.

2. ADVANCING RESPONSIBLE AI INNOVATION

Removing Barriers to the Responsible Use of AI

Cybersecurity and IT Infrastructure

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. 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.

Data

Ensuring access to high-quality and well-curated data for AI training and consumption is a work in progress. Legacy databases, data warehouses, and other data stores were designed based on requirements at the time and do not adequately reflect modern data management practices. Particularly, the use of data for AI was not contemplated or a prioritized requirement when designing and building our existing infrastructure. As a result, DOE faces obstacles in ensuring that data used for AI training and use in AI models is high quality, well-curated, and easily accessible. 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.

Internal Guidance for the Use of Generative AI

DOE developed and published the GenAI Reference Guide 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.

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 attracting, retaining, and training a workforce that will help the United States lead the world in AI innovation responsibly. To develop the next generation of AI talent, including in the federal government, DOE and the National Science Foundation (NSF) have established a pilot program to train 500 new researchers by 2025 to meet the rising demand for AI talent.

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 is now 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 Deference Cyber Workforce Framework to better identify the skillsets associated with those positions.

Additionally, the Department will provide resources and training to develop AI talent across its energy, environmental, and nuclear workforce and to also achieve AI literacy for non-practitioners to help ensure the responsible use of AI. DOE plans to leverage Office of Personnel Management (OPM)-provided gov-to-gov AI fundamentals training, the recently announced AI training series offered through the General Services Administration (GSA) AI Community of Practice, and the AI coursework available to employees in DOE's Learning Management System.

Further, DOE is prioritizing AI workforce hiring. FY26 IT budget guidance provided to DEs states that they should consider identifying a dedicated subject matter expert (or experts) to support rapidly evolving technologies, including GenAI. The AI expert would develop or support product development, ensure proper integration into existing technical environments, and collaborate on innovative initiatives.

AI Sharing and Collaboration

DOE developed a generative AI tool, PolicyAI, which is being researched within government agencies for searching and summarizing historical National Environmental Policy Act (NEPA) documents, for assistance in drafting new Environmental Impact Studies (EIS) to deploy new clean energy projects, for analyzing public comments, and for increasing access to public comment reviews. The investments in AI for permitting will augment existing research and analysis tasks for NEPA reviews while keeping a human in the loop for decision-making. DOE kicked off this initiative with 12 federal agencies.

DOE's Office of Scientific and Technical Information (OSTI) fulfills agency-wide responsibilities to collect, preserve, and disseminate both unclassified and classified scientific and technical information (STI) emanating from DOE-funded research and development activities. To serve this mission, 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 code with the public, as all DOE National Laboratories, facilities, and contractors are required to announce their software using DOE CODE. For sharing internally within the Department, DOE CODE offers a GitLab instance as a repository option for DOE-funded developers. Registered users can create and import their own repositories. The repository service can be helpful when developers need controlled access to code (e.g., not open source or not yet public), or for collaboration between developers from multiple labs or institutions.

Additionally, DOE's Office of Technology Transitions (OTT) 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.

Harmonization of Artificial Intelligence Requirements

DOE is engaged in the process of aligning AI guidelines and frameworks to reduce barriers, improve compliance, and foster innovation across the Department. The goal is to create a consistent set of guardrails that facilitate the development, deployment, and use of AI technologies while ensuring safety, security, fairness, and transparency. These aspects are being socialized across the Department using existing channels of communication, including working groups and standing cadences between leaders of from DEs and National Labs.

3. MANAGING RISKS FROM THE USE OF ARTIFICIAL INTELLIGENCE

Determining Which Artificial Intelligence Is Presumed to Be Safety-Impacting or Rights-Impacting

To ensure compliance with OMB guidance, DOE created the Rights- and Safety-Impacting AI Working Group. This group represents AI equities from across the Department and will support efforts to identify rights and safety impacting AI use cases. The group will first develop a checklist to guide the Department in determining if an AI use case is rights and safety impacting. This checklist will be shared with all Departmental Elements (DEs) 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 rights or safety impacting.

The Department also plans to develop AI policy communication roles and responsibilities for AI use. The policy will include a Contractor Requirements Document to levy the same minimum risk management practices on contractors developing AI use cases for the Department. Create a use case checklist for defining safety and rights impacting use cases.

During the annual AI use case inventory process, DEs will be asked to identify and report rights and safety impacting 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 Rights- and Safety-Impacting AI Working Group will provide recommendations on 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 rights or safety 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 Acting CAIO will determine if a waiver is appropriate, or if use case termination may be required.

Minimum Risk Management Practices

The DOE Rights-and Safety-Impacting 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 rights or safety impacting and confirm that the minimum risk management practices are implemented.