MEMORANDUM OF UNDERSTANDING
BETWEEN
THE U.S. DEPARTMENT OF ENERGY
AND
THE U.S. DEPARTMENT OF COMMERCE
As represented by
THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

CONCERNING COLLABORATIONS TO ADVANCE SAFE, SECURE, AND TRUSTWORTHY AI

This Memorandum of Understanding (MOU) is made between the U.S. Department of Energy (DOE) and the U.S. Department of Commerce, as represented by the National Institute of Standards and Technology (DOC). For the purposes of this agreement, DOE shall include the Department and the National Nuclear Security Administration (NNSA). DOE and DOC are collectively herein referred to as the "Parties" or individually as a "Party."

1. Background

DOE and DOC are both responsible for research and development activities to advance safe and trustworthy artificial intelligence (AI).

DOE supports basic and applied scientific research, including research on AI, related to its science, energy, and national security missions. DOE also has capabilities to test and evaluate the robustness, vulnerabilities, risks, and national security threats posed by AI. DOE has seventeen National Laboratories that tackle critical scientific challenges and possess unique instruments and facilities, many of which are found nowhere else in the world. DOE's National Labs operate four of the ten fastest supercomputers in the world and DOE's access to computing resources as well as comprehensive data sets across the physical and life sciences allow DOE to address large-scale, complex, multidisciplinary research and development challenges.

The National Institute of Standards and Technology (NIST), a Federal agency within the DOC, is the U.S. Government's leading institution for scientific measurement, including in AI and AI safety. NIST creates guidelines and supports development of voluntary consensus standards across a range of industries and sciences, and notably in AI risk management. NIST creates critical measurements solutions and promotes equitable standards to stimulate innovation, foster industrial competitiveness, and improve the quality of life. At the direction of President Biden and Commerce Secretary Raimondo, DOC has established within NIST the U.S. AI Safety Institute (USAISI or Institute) and the AI Safety Institute Consortium (AISIC or Consortium). The USAISI and AISIC were established to build a capability to perform direct evaluations of advanced AI models; do research on innovative methods in evaluation and other areas of AI safety and publish guidance to support the safe, secure, and trustworthy development and use of AI.

Executive Order 14110 *Safe, Secure, Trustworthy Development and Use of Artificial Intelligence* tasks the Secretary of DOC, acting through the Director of NIST, to coordinate with the Secretary of DOE to develop and help to ensure the availability of testing environments, such as testbeds, to support the development of safe, secure, and trustworthy AI technologies. Also under Executive Order 14110, the Secretary of Commerce, acting through the Director of NIST, is tasked with creating guidelines for agencies to evaluate the efficacy of differential-privacy-guarantee protections, including for AI; the Secretary of Energy is directed to fund the creation of a Research Coordination Network (RCN) dedicated to advancing privacy research and, in particular, the development, deployment, and scaling of privacy enhancing technologies (PETs); and DOE and DOC are directed to coordinate in supporting the design, development, and deployment of PETs.

2. Authority

DOE enters into this MOU under the authority of section 646 of the Department of Energy Organization Act (Pub. L. 95-91, as amended; 42 U.S.C. § 7256). DOC enters into this MOU pursuant to 15 U.S.C. 272(b), 272(c), 273, and 278h-1.

3. Objective/ Purpose

The Parties intend to collaboratively engage in the evaluation and/or creation of guidelines for evaluation of AI models, research into AI models and systems, and research and development of AI risk-mitigation tools and techniques, including AI PETs. AI models and systems are inclusive of open and proprietary frontier AI models and systems. Collaborative activities of the Parties may also include partnering on the evaluation of AI capabilities, limitations, risks, and impacts, as well as coordinating to establish and make available testbeds to support the development of safe, secure, and trustworthy AI technologies. These activities will be henceforth referred to as "AI Activities."

4. Proposed Areas of Collaboration

The Parties intend to explore, identify, and launch collaborations for AI Activities between DOC and DOE, including by leveraging the capabilities of the DOE National Laboratories and NIST's USAISI, AISIC, and laboratory programs.

5. Proposed Forms of Collaboration / Understandings of the Parties

The Parties intend to collaborate through mutual visits; the exchange of information; communication among evaluation performers, researchers, and experts; and planning for potential future joint research or other activities as the Parties may deem appropriate.

Staff from DOE's national labs and sites and NNSA's national labs, plants, and sites, at the direction of DOE or NNSA and as consistent with their Management and Operating Contracts, will participate in AI Activities. Information can be exchanged and discussed between NIST, DOC, DOE, and the national labs as needed to fulfill the objectives of this MOU. Participation in the activities of the AI Safety Institute Consortium by staff from DOE's national labs and sites and NNSA's national labs, plants, and sites will occur through a separate agreement.

a. DOE and DOC intend to:
    1. Jointly cooperate on AI Activities;

2. Hold regular coordination meetings to discuss ongoing activities and to plan for future engagements; and

b. DOE intends to:
    1. Facilitate the establishment of joint AI Activities between DOC and the DOE National Laboratories;
    2. Share with DOC information on available testbed resources suitable for AI Activities, including but not limited to large-scale DOE high performance computing resources and, subject to appropriate security clearances and a need to know, classified cloud-based testbeds. DOE will make its best effort within existing processes to accommodate requests from DOC for access to High Performance Computing and cloud-based testbed resources;
    3. Develop and evaluate PETs for scientific and technical use cases;
    4. Lead unclassified and classified evaluations of foundation and other AI models for radiological and nuclear threats and perform unclassified and classified evaluations for chemical and biological threats, both pre- and post-deployment, and, subject to security clearances and a need to know, as necessary and appropriate, read-in DOC personnel on classified outcomes and conclusions;
    5. Share information on capabilities, best practices, knowledge gaps, and red-teaming techniques and outcomes, as appropriate; and
    6. Develop AI Risk Management Framework (RMF) profiles, in coordination with DOC, for areas in which DOE and the DOE National Laboratories hold specific expertise, including areas relevant to scientific AI and for mitigating CBRN threats.

c. DOC intends to:
    1. Lead unclassified evaluations of foundation and other AI models for impacts on national security, public safety, economy, and society, including, but not limited to, chemical, biological, cyber, autonomy, and loss of control threats;
    2. To better enable agencies to use PETs, create guidelines for agencies to evaluate the efficacy of differential-privacy guarantee protections, including for AI;
    3. Conduct privacy and PETs research to inform and develop new guidelines;
    4. Lead negotiations with AI model companies for model access for evaluations by DOC and DOE;
    5. Share information on capabilities, best practices, knowledge gaps, and red-teaming techniques and outcomes, as appropriate;
    6. With feedback from DOE, the AISIC, and other stakeholders, continue developing scientific research and evaluation around AI risk management;
    7. Work with DOE Program Offices in interfacing with the DOE National Laboratories on AI Activities to ensure a uniform and shared understanding of ongoing and planned efforts; and
    8. Facilitate connectivity between external partner organizations (foreign governments, third-party evaluators, etc.) and DOE for the purposes related to the performance of AI Activities.

6. Proposed Mechanisms of Collaboration

To administer the implementation of this MOU, each Party has designated an assigned "Principal Coordinator" to facilitate and coordinate the collaboration hereunder. Each Party may change its "Principal Coordinator" with written notice.

Principal Coordinator for DOE: Helena Fu, Director of the Office of Critical and Emerging Technologies.

Principal Coordinator for DOC: Elizabeth Kelly, Director of the U.S. AI Safety Institute.

a. The Principal Coordinators intend to hold meetings as necessary to discuss matters related to the collaboration and the development of written agreements consistent within applicable law and regulations. In particular, the Principal Coordinators intend to communicate regularly on matters involving red-teaming and national security. The Parties anticipate that meetings between the Principal Coordinators will be held not less than annually and may occur with much higher frequency as needed.

b. The Principal Coordinators may delegate specific responsibilities under this MOU as deemed necessary for the efficient and effective execution of this MOU and will provide to each other written notice of such delegations, including the specific scope and time frame of the delegation.

7. Modification and Discontinuation

a. This MOU becomes effective upon the signing of both parties and will expire five (5) years from the effective date. Renewal of the MOU may be accomplished by written agreement of the agencies.

b. The Parties may discontinue this MOU at any time by mutual written consent. Alternatively, a Party that wishes to discontinue its participation in this MOU should provide notice of not less than thirty (30) days.

c. This MOU is not transferable except with the written consent of the Parties.

d. Consistent with the Purpose and Objective Section above, the scope of collaboration may be extended to other areas upon mutual written consent of the Parties and subject to all applicable laws, rules, and regulations.

8. Exchange of Information

a. The Parties intend to engage in the timely sharing of information relevant to the execution of AI Activities, including the following, as may be appropriate:
   i. Planning of strategies and approaches relating to the development or execution of joint AI Activities;
   ii. Requirements for access to testbeds or computational resources as may be necessary to accomplish joint AI Activities;
   iii. Evaluations of AI models, techniques, software, or systems.

b. The Parties intend to appropriately mark information prior to sharing to protect sensitive information. Information marking will be subject to all applicable agreements, laws, and regulations.
c. The Parties acknowledge that the exchange of proprietary and/or sensitive information under this MOU may occur, and in such an instance, the Principal Coordinators and their respective Offices of the General Counsel and/or Chief Counsel will be responsible for negotiating any agreement required to protect such information and limit its distribution.
d. The Parties intend to facilitate direct communication between their personnel. Communication with industry and other outside stakeholders may occur in connection with the Parties' effective execution of AI Activities, and the Parties intend to facilitate such communication with staff of both Parties, as necessary and appropriate. Any agreement required to facilitate such communications or protect the information disclosed therein will be negotiated by the Principal Coordinators and their respective Offices of the General Counsel and/or Chief Counsel.

9. Promotion

a. The Parties intend that within 30 days of signing, the MOU will be announced by joint press releases which highlight the roles and intended contributions, foreseeable at the time of signing, of DOE and DOC. The Parties further intend to maintain a website, or websites, highlighting the MOU and joint AI Activities undertaken.

b. The Parties agree that DOC will publicly describe, and highlight on relevant webpages and other informational material, DOE as a partner of the USAISI. Correspondingly, DOE will highlight the USAISI, DOC, and NIST as a partner in DOE's efforts in safety- and security-related research and evaluation of AI models, on relevant webpages and other informational material.

10. General Provisions

a. This MOU in no way restricts either of the Parties from participating in any activity with other public or private agencies, organizations, or individuals.

b. This MOU does not create any legally binding obligations between the Parties.

c. Each Party should conduct the activities contemplated by this MOU in accordance with all applicable laws, regulations, and other requirements to which it is subject, including, by way of illustration and not by way of limitation, export control laws and environmental, health and safety laws.

d. The conduct of cooperative activities contemplated by this MOU is subject to the availability of funding, personnel, and other resources. This MOU does not document nor provide for the exchange of funds, reimbursement, or manpower between the Parties nor does it make any commitment of funds or resources.

e. Each Party is to be responsible for the costs it incurs in participating in cooperative activities contemplated under this MOU. Each Party is responsible for supervision and management of its personnel.

f. Each Party should ensure the protection and minimization of use of any personally identifiable information viewed, used, or disseminated between or by the parties according to all Federal applicable laws, rules, and obligations.

11. Security

DOE technologies and programs will be protected under the guidance and oversight of DOE. DOC technologies and programs are protected under the guidance and oversight of DOC. NIST technologies and programs are protected under the guidance and oversight of NIST.

FOR THE DEPARTMENT OF ENERGY:

By: Geraldine Richmond

Name: Geraldine Richmond
Title: Under Secretary for Science and Innovation

Date: 07/22/2024

Place: Washington, DC

FOR THE DEPARTMENT OF COMMERCE:

By: LAURIE LOCASCIO Digitally signed by LAURIE LOCASCIO Date: 2024.08.22 14:13:17 -04'00'

Name: Laurie Locascio
Title: Director, National Institute of Standards and Technology

Date: 8/22/2024

Place: Gaithersburg, MD

By: Jill Hruby

Name: Jill Hruby
Title: Under Secretary for Nuclear Security
Administrator, National Nuclear Security Administration

Date: 08/16/2024

Place: Washington D.C.