UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
OFFICE OF THE DIRECTOR

December 9, 2024

Mr. Steven B. Lipner
Chair
Information Security and Privacy Advisory Board

Dear Chairman Lipner,

Thank you for your letter conveying the need for, and importance of, coordination of AI safety efforts across federal departments and agencies. I strongly agree with the spirit of your letter and want to assure you that staff at the National Institute of Standards and Technology (NIST) have been hard at work to coordinate our AI work within our organization, across the U.S. Government, and with efforts around the globe.

NIST planted the seeds decades ago for the scientific and technical advances that were essential for creating what is recognized today as Al. Likewise, we have long been committed to building our relationships with stakeholders and mobilizing the community behind this topic and its challenges. The strength and legacy of this community-centered scientific foundation in AI leaves NIST well-positioned to advance the measurement science of AI. Just this year, the U.S. AI Safety Institute (AISI) was established within NIST in recognition of the fact that research and measurement is what is needed to begin solving these Al-related challenges.

As part of NIST's whole-of-government approach to AI safety, the AISI recently announced the formation of the Testing Risks of AI for National Security (TRAINS) Taskforce, which brings together partners from Commerce, Defense, Energy, Homeland Security, CISA, NSA, and NIH to identify, measure, and manage the emerging national security and public safety implications of rapidly evolving AI technology. The TRAINS Taskforce will enable coordinated research and testing of advanced Al models across critical national security and public safety domains, such as radiological and nuclear security, chemical and biological security, cybersecurity, critical infrastructure, conventional military capabilities, and more. Each member will lend its unique subject matter expertise, technical infrastructure, and resources to the Taskforce and will collaborate on the development of new Al evaluation methods and benchmarks, as well as conduct joint national security risk assessments and red-teaming exercises. The TRAINS Taskforce is expected to expand its membership across the Federal Government as its work continues.

Under the National Security Memorandum on *"Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety. Security, and Trustworthiness of Artificial intelligence"* issued on October 24, 2024 (NSM on AI), NIST has been designated to serve as the primary point of contact for the U.S. Government with private sector AI developers to facilitate voluntary pre-

and post-public deployment testing for safety, security, and trustworthiness of frontier AI models. Under the NSM on AI, NIST is directed to communicate testing results and feedback, as well as any appropriate risk mitigations, to the respective model developers and NIST's interagency counterparts. As the primary point of contact, NIST fosters collaboration in the AI ecosystem by engaging with these federal partners on the design of AI model evaluations and in the performance of AI model safety testing. NIST will expand such collaboration internationally by engaging with the international network of AI Safety Institutes, the initial membership of which includes entities from the United Kingdom, the European Union, Japan, Singapore, South Korea, Canada, France, Kenya, and Australia. These activities cement NIST's role in leading the advancement of the science of AI safety.

I also appreciate the recommendations you shared for NIST to lead AI safety and security efforts in a way that is coordinated across the Federal Government. NIST believes that cooperation with a diverse group of stakeholders throughout the public and private sectors is vital to realizing our vision of the future for AI and our goal of consistent and clear recommendations that are not conflicting or duplicative. As such, NIST takes an open, transparent, and collaborative approach to developing our guidance. For example, NIST released the NIST AI Risk Management Framework (AI RMF) in 2023, which is a resource for organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems. The AI RMF's voluntary guidance was developed through a consensus-driven, open, transparent, and collaborative process that included a number of opportunities for public engagement, including multiple workshops. The NIST AI RMF has served a basis for more custom applications, including the recent profile by the U.S. Department of State, *"Risk Management Profile for Artificial Intelligence and Human Rights"* which is a practical guide for organizations-including governments, the private sector, and civil society-to design, develop, deploy, use, and govern AI in a manner consistent with respect for international human rights. NIST's Trustworthy & Responsible Artificial Intelligence Resource Center (AIRC) supports and operationalizes the AI RMF offers crosswalk documents and additional use case Profiles for the AI RMF. These resources intend to provide clarity on how the AI RMF can be used in specific domains and alongside other guidance. NIST will continue to provide supplemental materials to help communities with implementation, resources permitting.

Finally, one of my priorities as NIST Director has been strengthening U.S. engagement in international standards for critical and emerging technologies, including for AI. NIST staff participate in ongoing coordination with key international partners and standards development organizations to drive AI-related consensus standards, cooperation, and information sharing. As part of such engagements, NIST staff connect with departments and agencies across the Federal Government to prepare and align messaging as practicable. In 2019, the Interagency Committee on Standards Policy (ICSP), chaired by NIST, created the AI Standards Coordination Working Group (AISCWG) to facilitate the coordination of federal agency activities related to the development of AI standards and develop AI standards-related recommendations for the ICSP. NIST furthered the AISCWG's work with the 2024 release of NIST AI I00-5, "*A Plan for Global Engagement on Al Standards*," which outlines a broad plan guided by the principles set out in the AI RMF for global engagement on promoting and developing AI standards and includes specific, high-priority ways for the U.S. Government to implement the report's recommendations.

Again, thank you for your letter and the hard work, leadership, enthusiasm, passion, and dedication which you have exhibited in chairing NIST's Information Security and Privacy Advisory Board. We will take your recommendations into consideration as we continue to make progress in this space. If you have any questions, please do not hesitate to contact NIST ITL Director Kevin Stine.

Sincerely,

LAURIE LOCASCIO

Digitally signed by LAURIE LOCASCIO
Date: 2024.12.05 10:54:02 -05'00'

Laurie E. Locascio, Ph.D., NAE
Under Secretary of Commerce for Standards and Technology &
Director, National Institute of Standards and Technology

cc: The Honorable Alejandro Mayorkas
Secretary
United States Department of Homeland Security

cc: Shalanda D. Young
Director
Office of Management and Budget