Statement of Saif Khan

Senior Advisor to the Secretary for Critical and Emerging Technologies

U.S. Department of Commerce

Before the

House Committee on Energy and Commerce

December 13, 2023

Introduction

Chair Rodgers, Ranking Member Pallone, and distinguished Members of the Committee, thank you for the opportunity to testify about the Department of Commerce's (DOC) work related to artificial intelligence (AI). I want to thank the Committee for its continued support for DOC's AI-related activities.

DOC is proud to play a core role in the Biden-Harris Administration's comprehensive approach to AI across the federal government, including to implement President Biden's recent Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI. As this Administration has recognized, AI is a transformational technology that creates enormous opportunities, and DOC is committed to harnessing its benefits. At the same time, even the creators of this technology themselves are warning us of its profound risks, which we are working to mitigate.

Today, I'll give a summary of DOC's current efforts in AI. First, the Department aims to create a "race to the top" in AI safety, security, and trust. Second, we are addressing AI-related threats to our national security. Third, the Department is fostering an innovative, competitive, and informed marketplace for AI. And finally, we are examining ways to use AI for good to enhance the government's work.

Safety Research, Guidelines, Benchmarks, and Tools

The Department is taking several actions to ensure that we meet our nation's, and the world's, needs for safe, secure, and trustworthy AI.

DOC houses the National Institute of Standards and Technology (NIST or the Institute), the premier U.S. government body for advancing measurement science and standards. The Institute, in close coordination with external stakeholders, has an extensive history of crafting the metrics, measurements, benchmarks, guidelines, and tools needed to shape and standardize sociotechnical processes in industrial science and commercial technology.

Building on that long history, its stellar reputation as an expert body, and its strong external relationships, our Department, through NIST and with support from Congress, published the Artificial Intelligence Risk Management Framework in 2023. The Framework now has significant buy-in: it is celebrated by many stakeholders in the United States and beyond as one of the premier frameworks for managing the risk of AI during the development, deployment, and

use of AI. We are following up with additional resources for the implementation of the Framework, such as a companion resource for generative AI.

In November 2023, Vice President Harris and Secretary Raimondo announced the establishment of the U.S. AI Safety Institute (AISI) within the Department. The NIST-led Institute will facilitate the development of guidance for measurements and methodologies to enhance safety, security, and trust, and will provide testing environments to evaluate capabilities, risks, and impacts, particularly from the most advanced AI technologies. The Institute is also launching a consortium to work with partners in academia, industry, civil society, and non-profit organizations to advance its AI safety mission. We intend to build on NIST's long history of producing scientifically grounded definitions, metrics, and frameworks, which have informed domestic and international progress, for the common good.

Under President Biden's Executive Order on AI, the Institute will develop guidelines for evaluating AI models' capabilities, risks, and impacts, including guidance for AI red-teaming; provide testing environments; create guidelines relating to the detection and labeling of synthetic content; and develop a companion resource to the Secure Software Development Framework for generative AI. The Institute will also be a home for foundational research to support its mission. The AISI will also collaborate with the Department of Energy and the National Science Foundation to make testing environments available to support the development of safe, secure, and trustworthy AI technologies, such as for technology evaluations including AI red-teaming, as well as to support the design, development, and deployment of associated privacy-enhancing technologies. After completing the work assigned to DOC by the Executive Order, we intend for the Institute to remain the hub of U.S. government AI safety and trust research, guidance, standards, evaluations, AI red-teaming, and testing.

Additionally, under the Executive Order, DOC's Bureau of Industry and Security (BIS) will issue ongoing surveys to ask U.S. AI developers how they are developing advanced AI models and what they are doing to keep those models safe and secure.

Addressing Threats to National Security

The Department, through BIS, continues to implement and enforce our AI-related export controls and is regularly updating them to adapt to the fast pace of change in this area. These controls are carefully tailored to ensure that U.S. innovations are not used to undermine U.S. national security.

This October, BIS updated its rules limiting access to advanced semiconductors that are fueling breakthroughs in artificial intelligence and sophisticated computers that are increasingly critical to military applications. These updates are specifically designed to control access to computing power to limit the proliferation and development of next generation models and military AI capabilities, which could otherwise threaten the national security of the United States and our allies and partners.

We are also developing a proposed regulation on AI-related know-your-customer and notification requirements for Infrastructure-as-a-Service providers, which will enhance the Department's visibility into foreign actors' development of advanced AI using U.S. cloud services.

Innovation, Competition, and an Informed Marketplace

The Department of Commerce is an engine of policy creativity and has long steered government action as it relates to new technologies. We will continue to build on the Department's robust expertise in technology governance to study and issue reports on difficult policy questions related to AI, with the aim of facilitating an innovative, competitive, and informed marketplace. The Department, through the National Telecommunications and Information Administration (NTIA), is preparing to publish a report on AI Accountability, which will make recommendations for federal government action to increase transparency and accountability in AI. We believe that safety and transparency make adoption more likely.

The Department, through NTIA, will also soon issue a call for public input related to the benefits, safety and security risks, and policy options with respect to widely available model weights of dual use foundation models. NTIA's engagement with the public and our in-house expertise will form the basis for a report on this topic in the summer. We expect this report to become a foundational document for future government decision-making.

DOC, through the Patent and Trademark Office, will also issue guidance on inventorship for AI-assisted inventions, other considerations at the intersection of AI and IP, and a set of recommendations for executive action on copyright in coordination with the Copyright Office. While recognizing the role of the legislature and the courts in the realm of intellectual property, our policy work will aim to help clarify the intellectual property landscape as it relates to AI.

Using AI for Good

The Department is looking for safe, responsible uses of AI to enhance our work. This includes the National Oceanic and Atmospheric Administration (NOAA), which is working closely with our European partners on AI applications that are designed to allow more accurate extreme weather forecasting, including of river overflows and wildfires. NOAA is also exploring use of AI for the operation of uncrewed mapping systems, processing underwater surveys of marine mammal and fish populations, automated language translation of weather forecasts and warnings, and processing, interpreting, and utilizing observations from NOAA satellites and other sensors.

The Department is also working to structure, label, and in some cases publish our troves of data, from NOAA and from Census, which are some of the biggest repositories of data in the world, so that they can be used for beneficial applications of AI with appropriate protections for privacy and other important interests.

Conclusion

The Department of Commerce was designed "to develop new fields of profitable trade and foster old ones . . . to facilitate industrial development and promote commerce at home and abroad."

For more than a century, this Department has been the steward of American commercial power. We have provided fundamental research and essential guidance where needed by our industries. We have refined the science of measurements and metrics across disciplines. We have adjudicated intellectual property rights. We compile key statistics and data about the nation. Internationally, we have promoted our trade and controlled our exports, with the aim of enabling U.S companies to do business wherever they can, while protecting American interests where we must.

We will pursue that mission as zealously in AI as we have with other industries, technologies, and products. In doing so, we will keep in mind that to be adopted widely, used productively, and deployed globally, AI must also be safe, secure and trustworthy. With the continued support of Congress, the Department is committed to meeting the opportunities and challenges of AI, in close partnership with our partners inside and outside government. We look forward to working with the Committee on this critical issue.

Thank you, again, for the opportunity to appear before you today. I look forward to your questions.