Additional Questions for the Record
Saif Khan, Senior Advisor for Critical and Emerging Technologies, Department of Commerce
House Energy and Commerce Committee Hearing
"Leveraging Agency Expertise to Foster American AI Leadership and Innovation"
December 13, 2023

The Honorable Cathy McMorris Rodgers

1. AI has the potential to help identify new cyber threats, but it can also help adversaries and bad actors create more severe attacks. Recently, the Washington Post published an article about Chinese hackers targeting and infiltrating critical infrastructure computer systems. Can you discuss how the Department of Commerce is planning to use AI to help identify and prioritize AI-powered cyber threats, particularly those originating in China?
    a. How does the Department plan to coordinate with DOE and industry stakeholders to use AI to protect critical infrastructure?

RESPONSE: AI technologies have the potential to transform cybersecurity. They offer the prospect of giving defenders new tools that can address security vulnerabilities and potentially mitigate cybersecurity workforce shortages – even as they can enhance the capabilities of those seeking to target organizations and individuals through information technology and operational technology attacks.

The National Institute of Standards and Technology (NIST) within the Department of Commerce promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life. NIST contributes to the research, standards, measurements, and data required to realize the full promise of AI, while managing its risks, to enable American innovation, enhance economic security, and improve our quality of life. As a non-regulatory body, NIST prides itself on the strong partnerships it has cultivated with the public and private sectors. NIST seeks and relies on diverse stakeholder insights and feedback from government, industry, academia, and non-profit entities to develop and improve its resources. The collaborative, transparent, and open processes NIST uses to prioritize, develop, and carry out its research and to produce its guidelines result in more effective and usable resources that are trusted and, therefore, widely used by federal agencies, as well as private sector organizations of all sizes, educational institutions, and state, local, tribal, and territorial governments. Our inclusion of international experts and organizations in most of these processes means that NIST's work is more likely to help shape the way that others around the globe approach issues related to AI standards and guidelines. This enhances the opportunity for alignment. NIST's team includes some of the top AI and standards experts in the world. Our staff has multidisciplinary backgrounds from industry, government, and academia with deep experience in various aspects of science and engineering related to AI. Currently, NIST experts and researchers have several AI-specific security efforts underway to help address these challenges.

NIST regularly works with DOE and industry stakeholders involved in multiple critical infrastructure sectors to address cybersecurity issues through the National Cybersecurity Center

of Excellence. NIST would look forward to continued engagement and partnership on these AI related issues.

The Department uses several industry standard capabilities and shared services offerings from the Cybersecurity and Infrastructure Security Agency (CISA) to identify and share information about cybersecurity risks from threat actors, regardless of origination. We continually evaluate the capability of service providers to evolve as the threat actors leverage emerging technology, such as AI. The Department uses the National Institute of Standards and Technology (NIST) Risk Management Framework as part of its systems development process to analyze and prioritize cybersecurity risks. By leveraging this framework, the Department ensures repeatable and consistent implementation of security controls to protect our mission.

The Department's role in protecting critical infrastructure is also effectuated through publication of standards and guidance through NIST publications. DOE and industry stakeholders have the opportunity to provide comments and feedback to NIST in developing guidance in the use of AI to protect critical infrastructure.

2. During the hearing we discussed how the President has used the Defense Production Act (DPA). I highlighted how, historically, the DPA has been a tool to shape the domestic industrial base to respond to emergencies (such as serious military conflicts, natural disasters, and acts of terrorism). In response to my concern on how DPA is being used with respect to the AI sector, and such use may result in a permission-based approach to AI, you responded that the Commerce Department is using the DPA for AI as an information gathering exercise as opposed to regulation. However, I had a follow-up relative to the CHIPS program, which is an industrial policy initiative, and how the DPA might be used to support AI advancement.

   How can the DPA be used to support the CHIPS program, which can advance U.S. leadership on AI? Do you believe that the Administration has the authority under the DPA to waive permitting and other regulatory obstacles to bolster our semiconductor and microelectronics sector?

   Has the Administration analyzed whether DPA Title III's authorities on "without regard to the l imitations of existing law" allow this industrial policy project to be carried out?

   RESPONSE: Implementing the CHIPS Act efficiently and effectively is an economic and national security imperative. As you note, implementation will help lay the foundation for a secure semiconductor supply chain to power critical technologies including AI. With this in mind, we plan to implement the statute consistent with and using all available legal authorities. The availability of the Defense Production Act to bolster our semiconductor and microelectronics sector would need to be determined in consultation with other federal agencies, including the Department of Defense, and the specific circumstances upon which any such authority would be invoked.

3. Does the Department of Commerce have a generally accepted definition for what constitutes "artificial intelligence" that falls under its regulatory authority? If so, please provide these definitions.

RESPONSE: Per the President's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110, or AI EO), "[t]he term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. § 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action."

The Honorable Jeff Duncan

1. What is the Administration's policy on forced data localization, discriminatory burdens on cross border data flows, mandatory source code transfer and other policies the United States has always opposed?

   RESPONSE:

   The United States is committed to advancing a fair, inclusive, and innovative digital economy. The Administration continues to engage stakeholders – including both large and small companies in the technology and other data-intensive sectors as well as privacy, safety, labor, and human rights advocates, to ensure that we continue to address these types of policies with the most targeted approach. We work with our partners to chart a path forward that appropriately balances preventing illegal discriminatory practices with our digital trade policy priorities.

   The Administration continues the United States' long-standing support for the trusted free flow of data and an open Internet with strong and effective protections for individuals' privacy and measures to preserve governments' abilities to enforce laws and advance policies in the public interest.

   The Department of Commerce has several programs aimed at promoting the cross-border data flows that are essential to businesses across sectors. For example, we continue the work to implement the EU-U.S. Data Privacy Framework and its UK extension, expand participation in the Global Cross Border Privacy Rules Forum, and encourage international policies that promote the trusted free flow of data, consistent with our historical posture on these issues.

2. The Administration's AI executive order imposes requirements on dual-use foundation models that pose a serious risk to security, national economic security, national public health, and safety. What types of AI models fall within this definition and are they covered by the executive order?

   RESPONSE: Per the AI EO: "The term "dual-use foundation model" means an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters,

such as by: (i) substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons; (ii) enabling powerful offensive cyber operations through automated vulnerability discovery and exploitation against a wide range of potential targets of cyber attacks; or (iii) permitting the evasion of human control or oversight through means of deception or obfuscation. Models meet this definition even if they are provided to end users with technical safeguards that attempt to prevent users from taking advantage of the relevant unsafe capabilities." Such models are covered by at least the portions of the EO that reference dual-use foundation models, including 4.1(a)(i)-(ii), 4.2(a)(i), and 4.6.

3. The Administration's AI Executive Order directs Commerce to undertake a number of tasks, including implementing reporting requirements for dual-use foundation models and conducting a consultation on open source. How will the Department of Commerce ensure that the private sector has an opportunity to contribute to these initiatives?

RESPONSE: The Department of Commerce is committed to ensuring that external stakeholders are given robust opportunities to provide their feedback. For instance, companies' responses to the survey required under Section 4.2(a) of the Executive Order (EO) will inform our future approach to dual-use foundation models. The Department intends to release for comment the proposed regulation required under Section 4.2(c) of the EO. The Department has already held a workshop on the question of dual-use foundation models with widely available weights and plans to continue to engage the public as it produces the report required under Section 4.6 of the EO.

The Department is also seeking public input on several NIST taskings, with topics including differential privacy guarantees, generative AI risk management, synthetic content detection and labeling techniques, global engagement priorities, and red-teaming practices and guidelines.

The Honorable Dan Crenshaw

1. Mr. Khan, your department was required by Executive Order 14034 to report on legislative and regulatory solutions to address foreign applications, like TikTok and WeChat, that receive sensitive U.S. data. I haven't been able to get an answer from your department about what those recommendations were. And I'm not alone, I know Senator Rubio asked for these reports as well. Will you commit to releasing this review (sections 2b and 2c of Executive Order 14034) and addressing the flow of input data, which could potentially be used against the United States?

RESPONSE: Section 2(b) of the Executive Order 14034 instructs the Secretary of Commerce, in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, the Secretary of Homeland Security, the Director of National Intelligence, and other appropriate agency heads, to provide a report or series of reports to the Assistant to the President and National Security Advisor with recommendations to protect against the harm from the unrestricted sale of, transfer of, or access to United States persons' sensitive data and recommendations on additional executive and legislative actions to address the risk associated with connected software applications that are designed, developed, manufactured,

or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary. The Department of Commerce is committed to working with Congress to address these threats**.**

The Honorable Anna G. Eshoo

1. Research and development of powerful artificial intelligence (AI) requires three main ingredients—good data, computing power, and people. These resources are expensive and mostly held in the hands of a few large technology companies. This concentration means that most of the talent in America is prevented from participating in AI R&D. This reduces competition, limits the boundaries of innovation, and hampers our ability to develop safe and trustworthy AI. That's why I introduced the CREATE AI Act, bipartisan, bicameral legislation to fully authorize the National AI Research Resource (NAIRR) and provide these resources to all sectors of society, including, small businesses, startups, the medical community, academia, nonprofits, and the public sector. To develop AI that is safe, trustworthy, and responsible, we must democratize access to it and allow every sector of America to participate in its research and development. President Biden recognized the importance of the NAIRR and directed the National Science Foundation (NSF) to stand up a pilot program. For the record, please answer the following questions:
    a. From the perspective of the Department of Commerce (DOC), why is it important for Congress to fully authorize the NAIRR? How will providing access to these important resources to all sectors of society improve the research and development of safe and trustworthy AI? How will democratizing AI and diversifying AI R&D help the United States stay competitive and continue to lead in AI innovation?
    b. The success the NAIRR Pilot will depend significantly on the cooperation of executive agencies and the resources they can provide. How is the DOC cooperating with the NSF on the NAIRR pilot? What resources is the DOC committing to ensure it's successful?

    RESPONSE: A National Artificial Intelligence Research Resource (NAIRR) would provide researchers with new or expanded access to computational resources, high-quality data, educational tools, and user support with a modicum of government oversight. Given that these resources are critical for conducting many forms of cutting-edge AI R&D, the creation of a NAIRR would expand the ranks of talented researchers able to contribute to the development of safe and trustworthy AI in a collaborative environment. The democratization of access to AI in this way would fuel innovation and advance AI for societal good which includes as an end state maintaining if not improving the nation's lead in AI innovation and adoption. The DOC has committed NIST staff which has participated in the 12-member task force that developed the implementation plan for a NAIRR. Additionally, NIST is supporting the NAIRR pilot by providing expertise and guidelines for advancing trustworthy AI. Leveraging the NOAA Open Data Dissemination program, NOAA is supporting the development of datasets of interest available to the NAIRR user community, and the U.S. Patent and Trademark Office (USPTO) is working to provide access to rich datasets for AI training and will support public challenges to spur the development of novel data products.

2. President Biden's Executive Order on AI directs the National Institute of Standards and Technology (NIST) to develop best practices for managing sequence-of-concern databases to support customer screening undertaken by synthetic nucleic acid sequence providers. These best practices will be developed in part by engaging with industry and other relevant stakeholders.

    a. Does NIST have plans to create a best practice or standard that could eventually be required of companies by DOC or other agencies?

    b. Does NIST intend to ensure that such best practice or standard would adequately guard against the highest-consequence risks, such as those that extend beyond the current FSAP list?

    c. How does NIST intend to engage with HHS, the National Security Council, and the Office of Science and Technology Policy around the development of these standards?

    d. Does the AI Safety Institute plan to develop best practices or standards for gene synthesis screening or does NIST plan to develop these through some other process. And if so, how does NIST plan to engage with civil society in their development?

    RESPONSE: NIST plans to lead and contribute to the development of best practices and standards, including through engagement with the private sector. NIST does not have the authority to require the use of these best practices or standards, but through that private sector engagement, particularly in the voluntary consensus, pre-competitive space, the expectation is that companies would see added value in adopting the best practices and standards. Additionally, NIST will work with relevant agencies and entities to provide technical expertise, as appropriate.

    The concept of which sequences constitute the highest-consequence risks is constantly evolving. Pending funding availability, NIST intends to continue to support updating the current best practices and develop ways to address evolving risks.

    NIST is already coordinating with HHS, the National Security Council, and the Office of Science and Technology Policy, as well as other agencies, and will continue to engage with these other agencies.

    Some relevant standards for gene synthesis screening are already being developed in the International Organization for Standardization (ISO) and other standards organizations, and NIST will continue to work with those entities during development of any other best practices and standards.

3. President Biden's Executive Order on AI tasked DOC with using the Defense Production Act (DPA) to order companies developing foundation models to produce records of activities to train such models, ownership of weights, cybersecurity measures to protect those weights, and the

performance of the model in red-teaming exercises, including "prior to the development of guidance on red-team testing standards by NIST...the results of any red-team testing that the company has conducted relating to lowering the barrier to entry for the development, acquisition, and use of biological weapons by non-state actors." For the record, please answer the following questions:

a. Are companies prepared to conduct red-teaming for biosecurity risks and how can Congress ensure they are?
b. What would it require for the government to be able to properly assess the results of those red-teaming exercises?

RESPONSE: Under the voluntary commitments secured by the White House, fifteen companies have committed to internal and external red-teaming of models for a range of risks, including biosecurity risks. The companies have also committed to publicly report safety evaluations conducted to the extent that these are responsible to publicly disclose.

The Department of Commerce intends to gather additional information on this question, via our tasking under the EO. NIST's development of red-teaming guidance will also impact the analysis of companies' preparedness.

The U.S. AI Safety Institute and its Consortium will address an array of efforts to advance safe and trustworthy AI systems, including through work related to guidance, methods, skills and practices for successful red-teaming. The Department anticipates that these efforts can help foster an AI ecosystem in which red-teaming, including for priority risks such as biosecurity, is easier to understand and implement.

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 to be able to bring on additional staff, accelerate work on testing environments, fund joint research partnerships, support the coordination of private sector engagement in the Institute's work, and other mission-critical activities.

Assessments of the results of red-teaming exercises may require technical expertise, as well as domain-specific expertise. In some instances, such assessments may benefit from access to or ownership of other assets including computational resources, data, source code, and model weights, to validate and verify certain results.

The Honorable Debbie Dingell

1. Data overcollection refers to the practice of gathering more data than is necessary for a specific purpose or task. It happens when technology companies collect and store more and different types of data than they need to provide the product or service being purchased. This creates privacy concerns, security risks, compliance issues, and various other challenges. Mr. Khan, the proliferation of artificial intelligence (AI) systems and particularly generative AI systems incentivize companies to collect, process, and transfer user data unnecessary to provide a specific product or service. What steps is the Commerce Department taking to address these concerns?

RESPONSE: The Commerce Department is dedicated to driving the protection of individuals' privacy while maintaining data accessibility for beneficial and controlled uses through the implementation of privacy-enhancing technologies. Among several relevant efforts across the Department, NIST recently released for public comment draft guidelines for evaluating differential privacy guarantees, supporting one of NIST's assignments under EO 14110. Specifically, the draft guidelines are intended to help agencies understand how to evaluate promises made (and not made) when deploying differential privacy, including for privacy-preserving machine learning. NIST has also published a Privacy Framework to help external entities respect privacy. NIST has also administered Prize Challenges aimed to advance the science of privacy-enhancing technologies. Additionally, in response to the Federal Trade Commission's (FTC) Advance Notice of Proposed Rulemaking (ANPRM) on commercial surveillance, the National Telecommunications and Information Administration (NTIA) emphasized the importance of data minimization and purpose limitation requirements.

2. Mr. Khan, can you outline the ways in which comprehensive federal privacy legislation could serve to shield American families from the overcollection, and potential misuse of their personal data?

   RESPONSE: The Commerce Department is committed to harnessing the power of artificial intelligence for societal good while protecting people from its risks, which includes strong privacy protections. To better protect Americans' privacy, including from the risks posed by AI, the President has called on Congress to pass bipartisan data privacy legislation to protect all Americans, especially children, and the Department is eager to work with Congress and the interagency on this important issue.

   The Department is working to structure, label, and in some cases publish our troves of data, from the National Oceanic and Atmospheric Association (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. In January 2023, the Department, through the National Telecommunications and Information Administration (NTIA), issued a request for comments to address issues at the intersection of privacy, equity, and civil rights, and which will inform a report on whether and how commercial data practices can lead to disparate impacts and outcomes for marginalized or disadvantaged communities.

   On AI safety, experts in industry, academia, and government are still assessing how to best address risks relating both to misuse and vulnerabilities. The Department is in an intensive information-gathering phase. As we focus on safety, security, innovation, competition, privacy, equity, and intellectual property (IP)-related concerns, the Department's work will allow us to get the information we need to act responsibly.

3. Mr. Khan, can you elaborate on the importance of adopting a federal data minimization requirement to protect consumers?

   RESPONSE: According to the Principles for Enhancing Competition and Tech Platform Accountability, the Biden Administration supports "clear limits on the ability to collect, use, transfer, and maintain our personal data, including limits on targeted advertising. These limits

should put the burden on platforms to minimize how much information they collect, rather than burdening Americans with reading fine print. We especially need strong protections for particularly sensitive data such as geolocation and health information, including information related to reproductive health. We are encouraged to see bipartisan interest in Congress in passing legislation to protect privacy."