# WHITE HOUSE POLICY ON AI

# HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

DECEMBER 6, 2023

**Serial No. 118–80**

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
*oversight.house.gov* or
*docs.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
54–392 PDF WASHINGTON : 2024

## COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
MIKE WALTZ, Florida

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
JIMMY GOMEZ, California
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida
RASHIDA TLAIB, Michigan

---

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
RAJ BHARWANI, Senior Professional Staff Member
LAUREN LOMBARDO, Deputy Policy Director
PETER WARREN, Senior Advisor
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director

CONTACT NUMBER: 202-225-5051

---

## SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
*Vacancy*

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
RO KHANNA, California
STEPHEN F. LYNCH, Massachusetts
KWEISI MFUME, Maryland
JIMMY GOMEZ, California
JARED MOSKOWITZ, Florida
*Vacancy*

# C O N T E N T S


Page

Hearing held on December 6, 2023 ..... 1


## WITNESSES


Mr. Samuel Hammond, Senior Economist, Foundation for American Innovation
Oral Statement ..... 5
Dr. Daniel Ho, William Benjamin Scott and Luna M. Scott Professor of Law, Senior Fellow, Stanford Institute for Human-Centered AI, Stanford Law School
Oral Statement ..... 7
Ms. Kate Goodloe, Managing Director, BSA, The Software Alliance
Oral Statement ..... 8
Mr. Ross Nodurft, Executive Director, Alliance for Digital Innovation
Oral Statement ..... 10
Dr. Rumman Chowdhury (Minority Witness), Responsible AI Fellow, Berkman Klein Center for Internet & Society, Harvard University
Oral Statement ..... 12

*Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: docs.house.gov.*


## INDEX OF DOCUMENTS


* Comments on Proposed OMB Memo, Workday; submitted by Rep. Langworthy.
* Statement for the Record, U.S. Chamber of Commerce; submitted by Rep. Mace.
* Statement for Record, CTA; submitted by Rep. Mace.
* Statement for the Record, AFP ; submitted by Rep. Mace.
* Statement for the Record, NAM; submitted by Rep. Mace.
* Questions for the Record: to Dr. Chowdhury; submitted by Rep. Connolly.
* Questions for the Record: to Ms. Goodloe; submitted by Rep. Langworthy.
* Questions for the Record: to Ms. Goodloe; submitted by Rep. Connolly.
* Questions for the Record: to Dr. Ho; submitted by Rep. Langworthy.
* Questions for the Record: to Dr. Ho; submitted by Rep. Connolly.
* Questions for the Record: to Mr. Nodurft; submitted by Rep. Langworthy.
* Questions for the Record: to Mr. Nodurft; submitted by Rep. Connolly.

*Documents are available at: docs.house.gov.*

# WHITE HOUSE POLICY ON AI

**Wednesday, December 6, 2023**

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION
*Washington, D.C.*

The Subcommittee met, pursuant to notice, at 2:07 p.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Timmons, Burchett, Burlison, Connolly, and Lynch.

Also present: Representative Lee of Pennsylvania.

Ms. MACE. Good afternoon, everyone. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will now come to order, and we welcome you here this afternoon.

Without objection, the Chair may declare a recess at any time, and I recognize myself for the purpose of making an opening statement.

Good afternoon and welcome to this hearing on the Subcommittee on Cybersecurity, Information Technology, and Government Innovation.

Since the release of ChatGPT just over a year ago, it has become clear AI could soon disrupt nearly every facet of our economy and society from healthcare to warfare. And that is good news. AI is a triumph of American innovation.

It is also likely to boost business productivity, raise our standard of living, and lead to life-saving and life-extending medical advances.

But like any powerful tool, AI could be used to inflict great harm when it is used carelessly or by malicious actors. That is why we have explored the dark side of AI in this Subcommittee, the risk that AI-fueled cyber-attacks pose to our national security and critical infrastructure, the threats to data privacy, the ways child sexual abuse material can proliferate online via deepfake technology, and the risk of personal harm to individuals from unchecked algorithmic bias.

These risks and others, including the rise and use of AI to weaponize biotechnology, are addressed in the broad reaching executive order on AI that President Biden signed on October 30.

Two days later, OMB followed on with a draft guidance specifically governing Federal agency use of AI. A brief comment period on that guidance ended yesterday. So, this is perfect timing for this hearing today.

In the EO, the President invokes extraordinary emergency powers, under the Defense Production Act, to require companies to notify the government about the development of powerful new AI systems and to share safety testing results.

But for the most part, both the EO and the OMB guidance tasks Federal agencies with mitigating against the dangers of specific, high-risk, AI-use cases as opposed to regulating the technology itself. That is a critical distinction.

The AI genie is out of the bottle, and it cannot be put back in. Suppressing core AI innovation here in the U.S. will not stop China from advancing the technology on its own, and if we fall behind China in the AI race, all other risks seem tame by comparison.

And China, quite frankly, as you all know, is not far behind.

That is why our support measures in these documents that seek to spur the recruitment and retention of AI experts in both the private and public sector. Here in the Federal Government, we need employees who can responsibly partner with the private sector to procure AI systems that make our government smarter, smaller, and more effective.

I look forward to hearing your views from industry witnesses today concerning how the OMB AI guidance is likely to impact Federal agencies' uses of AI and the ability of businesses to work with the government to provide cutting-edge AI tools that are safe and reliable.

But no one can yet judge the impact of the EO or the guidance. For the most part they are just kick-starting a process. The EO tasks Federal agencies with a massive laundry list of roughly 150 action items to take over the next year and beyond.

Dozens of regulations and guidance documents will be issued. Every major agency and many minor ones are enlisted in the effort, so we in Congress will be watching closely as this process unfolds.

But I am a little skeptical of Federal agencies that will keep to the timetable of action laid out in the documents because their track record is pretty useless. After all, the draft OMB guidance on government use of AI we are discussing today was due, by law, from this Administration more than 2 years ago, for example.

With that, I will now yield to the Ranking Member for his opening statement.

Mr. CONNOLLY. Thank you, Madam Chairwoman, and welcome to our panelists to today's hearing where we are making the world better one hearing at a time.

A Qualcomm report published just last week estimates that the total economic benefit of generative AI amounts to roughly $6.1 trillion to $7.9 trillion. Hard to believe.

So, what does this AI-infused global economy look like, whatever the number?

We already know virtual AI assistants like Alexa and Siri. I use both. Lesser-known use cases include helping scientists develop clinical drugs to treat pulmonary fibrosis, defending bank cus-

tomers from identity fraud, and improving traffic congestion for communities across the globe.

With these incredible advancements, AI also brings risks. In 2017, for example, researchers set out to train an AI model to identify cancerous lesions using clinical images. While researchers initially hailed the experiment a success, they subsequently realized that their algorithm's diagnoses were not informed by the lesion in the photo but rather by the presence of a dermatologist's ruler used to measure particularly concerning skin lesions.

That error could have been clearly a matter of life and death.

The United States must continue to invest in AI R&D and address those issues to solidify itself as a global leader.

Ten years ago, machines struggled to reliably identify images. Today national militaries are using AI analysis for satellite imagery, to determine missile and artillery strikes.

AI has also grown its ability to understand and respond to language to the point where even Members of Congress are using ChatGPT.

Over the past 10 years, the private sector has invested $249 billion into AI development, and the world's top 5 AI companies are headquartered in the United States.

On the public side, the National Science Foundation has announced a $140 million investment to establish seven new National Artificial Intelligence Research Institutes and to advance a cohesive approach to AI-related opportunities and risks.

In addition, agencies like NIH invested $5.9 million into the University of Virginia to fund research into how artificial intelligence could support care for diverse populations.

These investments can be important, if not critical, but the AI race remains competitive. If the U.S. fails to continue to support investment in this technology, we will be left behind, particularly by China.

While traditional research and development tools like data and training models can improve technology, so can Federal Government leadership in setting standards, guidance, and regulatory frameworks.

Establishing clear and transparent rules of the road builds trust within the public and establishes user security and privacy protections.

AI regulatory frameworks around the world will reflect the values of their own governments and societies, and those national frameworks matter because they will influence future iterations of AI.

In China, for example, the government requires AI companies to uphold core Socialist values in providing services. It is essential, therefore, that the United States lead in AI governance or the Nation risks ceding foundational control to adversarial forces eager to influence the future of AI.

President Biden's executive order on the safe, secure, and trustworthy development and use of artificial intelligence, along with OMB's draft implementation guidance, do that.

These frameworks lead a comprehensive, society wide effort to ensure AI best serves and protects the American people. The President's EO builds on the important action that this Administration

has taken on AI to date, including the creation of the blueprint for an AI Bill of Rights and the National Institute of Standards and Technology's AI risk management framework.

As the representative of the Silicon Valley East, I support provisions in the EO to bolster our Federal AI workforce. The President's accelerating hiring of AI professionals, while simultaneously offering AI training for employees at all levels of relevant fields, so the agency personnel are ready to confront the challenges both today and tomorrow.

President Biden's executive order and OMB's draft implementation guidance are essential documents for implementing this technology safely and responsibly across the Federal Government and society broadly.

Congress, industry, and the Administration must now work together to ensure that the Nation meets the important goals of the executive order and to continually seek to find and measure improved regulatory thresholds as needed as this technology evolves.

This Subcommittee looks forward to working with all stakeholders to encourage the safe and responsible development and usage of AI.

With that, I yield back.

Ms. MACE. Thank you.

I am pleased today to introduce our witnesses for today's hearing. Our first witness is Mr. Samuel Hammond, Senior Economist at the Foundation for American Innovation;

Our second witness is Dr. Daniel Ho, professor of law and senior fellow at the Stanford Institute for Human-Centered AI at Stanford Law School;

Our third witness is Ms. Kate Goodloe, Managing Director at BSA, the Software Alliance;

Our fourth witness is Mr. Ross Nodurft, Executive Director at the Alliance for Digital Innovation;

And our fifth and final witness is Dr. Rumman Chowdhury, a responsible AI fellow at the Berkman Klein Center for Internet and Society at Harvard University.

We welcome you all here today, and we are pleased to have you this afternoon.

Pursuant to the Committee rule 9(g), the witnesses will stand and raise their right hands, please.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth so help you God?

Let the record show the witnesses all answered in the affirmative. We appreciate all of you here today and look forward to your testimony. I will remind the witnesses that we have read your written statements, and they will appear in full in the hearing record. Please limit your oral statements to 5 minutes today.

As a reminder, please press the button on the microphone in front of you so that it is on when you speak, and the Members up here can hear you.

When you begin to speak the light in front of you will turn green. After 4 minutes the light will turn yellow. When the red light comes on, your 5 minutes have expired, and I will bang the gavel to shut you up. Just kidding. But I will.

So, today you all can take a seat. I would like to recognize Mr. Hammond for your opening statement for 5 minutes, please.

**STATEMENT OF SAMUEL HAMMOND**
**SENIOR ECONOMIST**
**FOUNDATION FOR AMERICAN INNOVATION**

Mr. HAMMOND. Thank you, Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee. My name is Samuel Hammond. I am the Senior Economist at the Foundation for American Innovation. We are a group of technologists and policy experts working to develop technology, talent, and ideas for a free and a more abundant future.

From the printing press to the internet, history shows that transformative technologies are a key driver of institutional change and evolution. Artificial intelligence is no different. The only question is whether our government will keep up and adapt or become overwhelmed by the pace of change.

This is why I believe the risk from adopting AI in government must be balanced against even greater risks associated with failing to adopt AI proactively enough.

Enter the White House's executive order on AI. A sprawling document, there is much to applaud in the executive order, from the streamlining of uses to attract and retain immigrants with AI expertise, to new initiatives for addressing Federal cybersecurity vulnerabilities.

I was particularly impressed by the EO's focus on, quote, dual-use foundation models such as those that can be used to generate biologic agents, cyber weapons, or other catastrophic hazards to the American public.

The EO requires basic disclosures from large computing providers and the adoption of minimal safety testing for future, more powerful AI systems.

Yet more than anything, the bulk of the executive order is aimed at promoting the use of AI within government. Whether it is successful, only time will tell as right now it is mostly a series of requests and reports.

My worry, though, is that it does not go far enough and could even hinder the fulsome adoption of AI in government given excess focus on hypothetical harms and even deeper failure of imagination.

Our institutions and AI are in an arms race, and we need to sprint just to stay in place. This is most obvious in the arena of cybersecurity where AI is both creating novel threats and more powerful forms of cyber defense.

Yet these arms-race dynamics extend far beyond cases where AI is explicitly misused. Even the most productive uses of AI will put unprecedented strain on our government.

Just last week Google DeepMind published an AI model that discovered 380,000 new stable materials. This represents nearly 800 years' worth of new material science knowledge achieved virtually overnight.

Now imagine what will happen when the same pace of change comes to medicine as it almost surely will. Is the FDA prepared to

handle an order of magnitude increase in new drug discovery? The answer is clearly no, at least not under business as usual.

Similar bottlenecks exist through the Federal Government. In every case managing the AI transition will require government to not only adopt AI aggressively but may even force Congress to rethink the configuration of our administrative and regulatory agencies from the ground up.

From broken procurement policies and cumbersome procedures, incremental reform is unlikely to suffice. We must modernize government at the firmware level and embrace AI and AI frameworks that truly scale, or risk government becoming the primary bottleneck to technological progress.

Earlier this year OpenAI published a paper assessing the likely labor market impacts of large language models. They found jobs like accountants, auditors, and legal secretaries face an exposure rate of 100 percent.

Many large companies have already begun downsizing, or have plans to downsize, in anticipation of the enormous efficiency gains unlocked by emerging AI tools and AI agents.

Much of the work performed in government bureaucracies is similar low-hanging fruit for AI. Congress should request an analogous survey to discover which Federal jobs are most exposed to AI automation or augmentation and to what extent legislation is needed to enable new, AI-enabled models of governance.

The goal should not be to downsize the Federal Government, per se, but rather to augment productivity and free up human resources for higher-value uses.

Given bureaucratic inertia, it is not enough to simply ask agencies to prioritize use of AI in government. Congress must push the Federal Government to adopt AI more aggressively, including by authorizing additional AI training resources, hiring authorities, and nimble funding for modernization.

The same tools for enhancing Federal capacity can be further used to strengthen congressional oversight. As agencies embrace AI internally, managers will be able to easily track and query the performance of their staff, automatically generating reports and work summaries from common document repositories.

These same techniques could be used to expedite reports to Congress and even enable near real time monitoring of an agency's activities. You could call it an Inspector General GPT.

Innovating within government should mean more than just plugging AI into some existing outdated process and calling it a day. We need true inventiveness and ambition. So, while White House has taken some important first steps, there is much more to be done.

Thank you and I look forward to your questions.

Ms. MACE. Thank you.

I will now recognize Dr. Ho to begin your opening statement.

**STATEMENT OF DANIEL HO**
**PROFESSOR OF LAW AND SENIOR FELLOW**
**STANFORD INSTITUTE FOR HUMAN CENTERED AI**
**STANFORD LAW SCHOOL**

Dr. HO. Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thanks for this opportunity to testify today.

There are three possible futures of AI. One is a future of AI abuse unchecked by government regulation. Nefarious actors use AI voice cloning to scam citizens, bot-generated texts to impersonate people, and deepfakes to erode trust.

Another is a future where the government harms citizens because of improper vetting of AI.

But a third future is possible where the government protects Americans from bad actors and leverages AI to make lives better, like the VA's use of AI to enable physicians to spend more time caring for veteran patients and less time taking notes.

To get to that future, we must make the right decisions today. The AI EO and OMB memo are important steps. Their focus on AI safety, investment, talent, and leadership are critical for America to lead in AI innovation and governance.

But the executive branch cannot achieve this goal fully without Congress. By our count, as Chairwoman Mace noted, the EO has some 150 requirements with urgent deadlines.

Based on my research of prior AI-related EOs, the government needs sufficient resources, expertise, information, and flexibility to realize this vision. I, therefore, recommend six actions.

First, Congress should support the EO's focus on top-level leadership from the White House and from the agency chief AI officers. Agencies will need resources and flexibility to not just put out fires but craft long-term strategic plans.

Second, Congress must support efforts to A, attract, train, and retain AI talented America; and B, provide pathways into the public service. Each year our universities are turning out a growing number of students with advanced degrees in AI. Yet fewer than 1 percent of AI Ph.Ds. pursue a career in public service. We need creative public-private partnerships to fix this talent gap.

When the return of millions of overseas veterans after World War II threatened to overwhelm the VA hospital system, the VA developed a pipeline of medical students and faculty to provide veteran care.

At Stanford RegLab and HAI, we collaborate with government agencies to prototype exactly this kind of partnership in AI, and increasing mechanisms to partner and collaborate with universities will be critical.

Third, a mandated, adverse event reporting system that requires parties to disclose AI harms would equip the government with information to ensure that AI is safe for the American public. Chairwoman Mace, for instance, has called for exactly this kind of information.

Some calls for regulation have been driven by more speculative risks, such as how ChatGPT might facilitate bioweapons. Other harms are very real, such as erroneous loan denials, biased hiring algorithms, or malfunctioning self-driving cars.

Currently our government lacks unbiased information. Adverse event reporting, like what already exists for cybersecurity or medical devices, would ensure that the government can tell fact from fiction about real and emerging AI harms, and it would enable targeted regulation that avoids stifling innovation.

Fourth, the development of general-purpose foundation models should not be restricted through a licensing regime. Fears about the capabilities of these models have led some to argue that foundation models should only be developed by a few well equipped companies.

This is wrong. Licensing only a small number of companies would impede valuable safety research. The most important forms of accountability come from oversight by many.

Done poorly, licensing would concentrate power, limit competition, and exacerbate the information gap between government and industry.

Fifth, government must appropriate funds to agencies and pass the bipartisan CREATE AI Act to fully authorize the National AI Research Resource and foster investment in R&D necessary for a wider range of Americans to participate in the AI revolution.

The National Institute of Standards and Technology is tasked with establishing the U.S. AI Safety Institute to develop verifiable and enforceable safety standards. Agencies like NIST must be sufficiently resourced to carry out these critical missions.

Sixth, government innovation should not be trapped in red tape. The OMB memo is exemplary in spelling out the opportunities and risks of AI, but process must be tailored to risk.

For instance, the memo's proposal that agencies allow everyone to opt out of AI for human review does not always make sense given the sheer variety of programs and uses of AI.

Since 1965, the U.S. Postal Service, for instance, uses AI to read handwritten zip codes on envelopes. Opting out of this system would mean hiring thousands of employees just to read digits alone.

Humans also make mistakes. Denials of SNAP benefits, for instance, are inaccurate 44 percent of the time. The government cannot "human" its way out of these problems. The government must build and leverage AI systems that complement human strengths and values.

In sum, the AI EO and OMB memo have taken a big first step, but it is only one step on the longer journey. Congress must now take it.

Thank you and I welcome your questions.

Ms. MACE. Thank you.

I now recognize Ms. Goodloe to please begin your opening statement.

**STATEMENT OF KATE GOODLOE**
**MANAGING DIRECTOR**
**BSA, THE SOFTWARE ALLIANCE**

Ms. GOODLOE. Good afternoon, Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee. My name is Kate Goodloe, and I am Managing Director at BSA, the Software Alliance.

BSA is a leading advocate for the global enterprise software industry. BSA members are at the forefront of developing cutting-edge services, including AI, and their products are used by businesses in every sector of the economy and by agencies across the Federal Government.

I commend the Subcommittee for convening today's hearing, and I thank you for the opportunity to testify.

The United States needs a strong, clear, thoughtful approach to AI policy. Both Congress and the Administration have important roles in developing that policy. It is critical for the United States to get this right.

The benefits of AI are clear, as companies of all sizes in every industry use AI to improve safety, create better products, and serve their customers.

There are also significant risks if AI is not developed and deployed responsibly. AI policy should, one, protect individuals from real risks by creating durable safeguards that promote trust in AI; two, enable the government to benefit from AI technologies and deliver better public services; and three, position the United States as a leading voice in the global approach to responsible AI.

The benefits of getting this right are significant, including to promote the government's ability to procure and use tools like AI-powered cybersecurity services.

Think about a Federal agency trying to protect both its network and the sensitive information it has about individuals, things like passport information, medical records, tax documents.

We already know bad actors are using AI to launch increasingly sophisticated cyber-attacks. The government needs AI to stay ahead of those threats too.

The United States' AI policy should support important beneficial uses of AI that improve health, safety, national security while creating guardrails for high-risk uses.

The recent executive order takes an ambitious whole-of-government approach to AI policy. I want to highlight several of the positive steps it takes to advance responsible AI.

The executive order recognizes the importance of the AI risk management framework developed by the National Institute of Standards and Technology. We encourage the Administration to ensure that framework anchors the government's risk management efforts.

The executive order also recognizes the importance of AI in cyber defense. It launches a pilot program to implement the National AI Resource to give researchers access to compute power and training resources.

It recognizes the importance of content authenticity, tools, and standards to help people know when content is real and when it has been altered, and it promotes the coordinated enforcement of civil rights statutes across agencies.

Other parts of the order create notable, important obligations with effects that will depend on how they are implemented. We encourage the Administration to consult with stakeholders, including industry, to ensure those obligations work in practice and do not undermine the order's goals.

I will give two examples. First, are new reporting requirements, which will apply to companies that develop certain potential dual-use foundation models and entities that acquire or possess large scale computing clusters.

Second, are new know-your-customer obligations for U.S. infrastructure-as-a-service providers, who must report certain transactions with foreign persons to the Department of Commerce and pass on those obligations to their foreign resellers.

The executive order also addresses government use and procurement of AI which are the focus of the draft guidance by the Office of Management and Budget. My written testimony includes BSA's recommendations for improving that guidance, including to ensure it applies consistently across agencies.

It is also important to coordinate OMB's changes with five concurrent regulatory updates that affect how the government procures AI. Failing to do so can undermine the government's goal of effectively leveraging AI.

The executive order is much broader than these efforts. It tasks more than 40 Federal agencies and entities with drafting reports, conducting consultations, and developing rules.

Despite this ambitious approach, the order does not replace the need for congressional action on AI. Congress should play a leading role in setting the United States' AI policy in at least two ways.

First, Congress should pass legislation that ensures the NIST framework guides the government's use and procurement of AI systems.

Second, Congress should enact legislation that establishes new safeguards for private sector companies that develop and deploy high-risk AI. These actions can help to create a strong, clear, and thoughtful United States AI policy.

Thank you for the opportunity to testify, and I look forward to your questions.

Ms. MACE. Thank you.

I will now recognize Mr. Nodurft for your opening statement.

**STATEMENT OF ROSS NODURFT**
**EXECUTIVE DIRECTOR**
**ALLIANCE FOR DIGITAL INNOVATION**

Mr. NODURFT. Thank you, Chairwoman Mace, Ranking Member Connolly, and Members of the Committee for holding this important hearing today. My name is Ross Nodurft. I am the Executive Director for the Alliance for Digital Innovation. We are a coalition of innovative commercial companies whose mission is to bring IT modernization and emerging technologies to the government.

My prior experience includes working at the Office of Management and Budget, in the Office of the Federal Chief Information Officer, as well as working in the private sector with many companies to modernize their technology, bring in Cloud services, cybersecurity products, and now artificial intelligence tools.

As the Executive Director of the Alliance for Digital Innovation, I represent leading technology, artificial intelligence, quantum computing, cybersecurity, and professional service providers, all working with the public sector.

ADI focuses on four key areas in our advocacy efforts—accelerating technology modernization in government, enabling acquisition policies that make sense to bring in innovative technologies, promoting cybersecurity innovations to better protect the public and the private sector, and then improving the public sector's technology workforce.

Regarding the Administration's recent AI policies, overall, ADI is supportive of any legislation or administrative policy that promotes adoption and use of modern Cloud-based commercial technology to increase the pace of government mission delivery.

We are also very supportive of the efforts to provide a public comment period for a draft memo. We understand that that is not something that is done traditionally, and we really support that effort.

However, there was a really short turnaround time that is limiting the amount of thoughtful and constructive feedback that industry can provide.

In fact, the rushed nature of the response mean OMB will be finalizing its guidance to agencies without the full benefit of insights that can be provided by the industry partners that are developing and deploying the AI capabilities in partnership with the government.

That said, ADI believes there are several important key areas that the administration should clarify as it updates its guidance.

The OMB memo could inadvertently keep innovative businesses away from the public sector. The OMB memo creates a series of fractured and unevenly administered new processes across departments and agencies that will deter many companies, including small and midsize technology companies, from working with the Federal Government.

To solve for this, OMB should provide additional specificity about various trigger mechanisms for determining which technologies are considered rights-impacting and which technologies are considered safety-impacting.

It should create a repository for the reuse of various products or testing documents.

And then they should consider certain use cases, like specific cybersecurity-use cases, to call out as neither rights-impacting, nor safety-impacting, and proactively exempt those products and services from the minimum requirements.

Government should use current government processes for AI. We cannot have agencies trying to implement the new processes without fully considering how they fit into current technology and security governance regimes, and how they are optimized for AI adoption.

We strongly encourage the Administration to provide agencies with enough time to optimize their plans for adoption and use of AI, leveraging current governance processes before providing their plans to comply with the executive order.

The government should prioritize specific AI-use cases. AI technology is not new. It has been around in many forms for many years. ADI believes that OMB must help agencies prioritize governance processes that focus on delivery of new AI or generative AI capabilities and to distinguish from those existing AI and machine

learning capabilities that are already authorized and in use in the Federal Government.

The government must refine definitions and trigger mechanisms for rights-and safety-impacting systems. ADI recommends further refining safety-and rights-impacting definitions to delineate harms associated with specific categories.

Examples for safety-impacting could be loss of life or serious physical harm, while rights-impacting examples could be tied to harms that are currently protected by existing laws such as non-discrimination and consumer protection.

In addition to further defining the risks, ADI believes that OMB must better define the term "meaningful impact" which acts as the trigger mechanism for such harms.

Finally, the government should clarify data ownership and focus on outcome-based testing. OMB should clearly state that the company data and proprietary, personal information does not have to be disclosed to the government for review.

Additionally, OMB should clarify that assessing the quality and the appropriateness of relevant data does not mean reviewing the underlying training data when reviewing AI systems but instead allows for a summary description of the characteristics of the training design data and ensuring that that will meet the requirement.

Finally, ADI recommends that OMB focus on model testing, known limitations, guidelines for intended use, and example-performance results of an AI model.

Thank you again to the Committee for the opportunity to testify, and I look forward to your questions.

Ms. MACE. Thank you.

I will now recognize Dr. Chowdhury to please begin her opening statement.

**STATEMENT OF DR. RUMMAN CHOWDHURY**
**RESPONSIBLE AI FELLOW**
**THE BERKMAN KLEIN CENTER FOR INTERNET AND SOCIETY**
**HARVARD UNIVERSITY**

Dr. CHOWDHURY. Chairwoman Mace, Ranking Member Connolly, and esteemed Members of the Committee, my name is Dr. Rumman Chowdhury, and I am a data scientist and social scientist who has built AI, and responsible AI, within and without industry for the past decade.

The executive order and the subsequent OMB guidance lay out an ambitious strategy for the accelerated responsible deployment of AI.

I applaud the recognition that, in order for the U.S. to remain an AI superpower, it must focus on safe, secure, and trustworthy use. I offer the following recommendations to facilitate this goal.

First, the U.S. must remain an active leader in the global AI landscape by funding targeted interventions and responsible AI for public and global use;

Second, in order to achieve the goals of section 4 of the EO, support and fund NIST;

Third, develop the independent community of algorithmic auditors by enabling secure-model access and investing in education for

structured, public feedback methods such as red-teaming and bias bounties;

Fourth, develop a minimum requirement standard that includes a determination of whether or not AI adoption is necessary and appropriate for Federal Government use.

First, countries are moving quickly to establish global standards and best practices around responsible use. I arrived this morning from Singapore's AI for Global Good workshop.

Their government gathered AI experts from around the world to help co-create ten projects that they will fund for open use and global benefit.

They are not alone. I have collaborated on similar efforts in London, Brussels, Paris, and Oslo, where there is similar investment in global, responsible-use best practices.

The U.S. must continue to set global AI priorities in alignment with section 11 of the EO. I recommend that the government similarly invest in public interest projects for responsible use that are open access, publicly available, and drive as a resource for individuals around the world.

Second, simply put, support NIST. Section 4 of the EO develops an ambitious strategy to leverage the institutional authority and capacity of NIST and expand their remit. I can think of no better team to execute on this plan.

With a limited timeline and broad scope, they require significant funding and resources to deliver the global, standard-setting quality that NIST is known for.

Similar institutes are funded accordingly. The U.K. AI Safety Institute has 100 million pounds earmarked for their endeavors. The Norwegian Government has allocated a 1 billion kroner fund toward AI development.

In addition, the proposed U.S. AI Safety Institute must remain housed as NIST. As a scientific measurement body, they provide much needed empirical evidence data to help us understand and prioritize how we address the risks and harms introduced by AI systems.

The U.S. Safety Institute must focus on a wide range of harms—societal impact, bias and discrimination, as well as broader considerations of future risks—in order to provide the full breadth of assurance we need to safely deploy AI. We already have significant evidence of AI systems in use today that infringe upon basic civil and human rights.

Third, in June, I testified to the House Science, Space, and Technology Committee on the topic of AI. At that time the concept of red-teaming was known by cybersecurity and few others.

Since then, it has become a topic of much consideration, mentioned 15 times in the EO alone. This is due, in part, to the White House's support of the generative AI red-teaming exercise this past August, which was co-led by my organization, Humane Intelligence.

We need to continue that momentum and enthusiasm. Newly appointed chief AI officers, as required by the draft OMB guidance, should engage with trusted organizations, including the Safety Institute, as well as independent external organizations to develop red-teaming as a part of standard vendor procurement and project-evaluation processes.

Fourth, AI is often a hammer in search of a nail. We cannot assume that AI is always the best answer to a problem as developers optimize for efficiency rather than effectiveness.

We have already seen how the use of AI infringes upon civil rights by algorithmic discrimination in criminal justice, employment, banking, and more.

In 1971, the Supreme Court addressed a similar problem—unintentional employment discrimination introduced by aptitude tests. The Griggs v. Duke Power Company ruling enabled the disparate impact requirement that is today widely used in evaluating AI hiring systems.

In order to achieve the goals of sections 7 and 8 of the executive order, I recommend a similar approach for the use of AI in high-risk situations in order to mitigate unintended consequences due to algorithmic bias.

A minimum standards test could include the following: A determination of whether or not an AI system performs better than an equal investment in improving the current system; requiring alignment with impact metrics designed with NIST to measure the effectiveness and robustness of the system, not just performance efficiency; a strategy to proactively identify and address real-world biases and adverse outcomes through in-context testing methods like expert or public red-teaming.

In conclusion, we must be circumspect on if, when, and how we adopt AI systems. This technology is meant to serve humanity, and innovation is only possible if we are all able to reap the benefits.

Thank you for your time.

Ms. MACE. Thank you so much.

I now ask unanimous consent to enter into the record three letters from the following organizations: Americans for Prosperity, Consumer Technology Association, and the National Association of Manufacturers.

And without objection, so ordered.

Ms. MACE. Thank you. I will now recognize myself for 5 minutes of questioning.

My first question is for you, Mr. Hammond.

The biggest risk concerning government use of AI is that it will not happen fast enough, like everything. I mean, today we still have legacy systems throughout the Federal Government, and we are all asking ourselves why.

Call me a little bit of a skeptic. I mean, I learned COBOL 25 years ago, and we are still using it in the Federal Government. But according to your written testimony today, it states the question is whether governments will keep up and adapt or be stuck riding horses while society whizzes by in a race car.

So, could slow and reluctant government adoption of AI jeopardize the cybersecurity of Federal systems? Is this a national security issue? Where do you see it?

Mr. HAMMOND. Well, thank you for your question. Yes, I think it is both a national security issue and a sort of good-government issue. So, you mentioned COBOL. We lived through the pandemic, and when you saw those line-ups around the block to claim unemployment insurance, a big part of that was because state unemploy-

ment insurance systems are built on mainframe computing technology from 50, 60 years ago.

It is broader than that as well. You know, look at the IRS. The IRS individual master file, which is sort of the core file that determines individual and business tax returns, was coded in assembly. So, even more primitive than COBOL, it was from the Kennedy Administration.

And so, these systems, in addition to cybersecurity, present sort of risks from through-put in denial of service. So, you know, I give an example of, you know, what happens when there is another sort of net neutrality style debate where activists on both sides are submitting regulatory comments. But now instead of just being expletives, they are fully cogent, well written comments that under the Administrative Procedures Act, we all have to read and respond to.

Those kinds of sort of tsunamis of information, even if they are not explicitly misused, could easily overwhelm an agency. And so, you know, in that case, maybe we need to adopt AI for summarizing comments or something like that.

I also think of this in the context of information requests. So——

Ms. MACE. Or filtering data is another, you know, way to do that as well—sorry to cut you off because we are at 3 minutes now.

I would like to ask a question of Dr. Ho. You have written about the lack of AI talent in government and the failure of this Administration to timely implement AI-related mandates.

I think you said in your testimony like 1 percent of AI qualified—people qualified in AI are in the public service—public sector.

So, under this new EO, it has got 150 new tasks to perform based on your count. Do you expect Federal agencies to meet the timetables for actions set out in the EO?

Dr. HO. Thank you, Chairwoman Mace. I think you are right, that earlier work showed that the two prior AI EOs were inconsistently applied, and I think what is good to see about this EO is that the Administration has really learned from some of the documentation and weak points, particularly in terms of providing clear definitions, having some people in charge at each agency.

And the question you raise is a really important one, and this Subcommittee has been so important in really providing good oversight and transparency over implementation.

I think followup is going to be necessary, and I think the talent pipeline that you mentioned is going to be absolutely critical for ensuring that the right folks are in place to be able to implement these requirements faithfully and in an informed way by the technology.

Ms. MACE. Thank you. And then my last question will go to Mr. Nodurft and Ms. Goodloe.

By farming out so many decisions to individual agencies, are either of you worried about the EO and the guidance might lead to multiple, conflicting, AI-enforcement regimes within the government? How is that going to work? What does that look like to you?

Mr. NODURFT. So, that is one of my bigger concerns here. There is a lot of emphasis—and the risk decisions and risk management is at the agency level, and it should be. And there are very specific use cases for every AI deployment.

That said, there is a gap between the guidance that is currently being provided and the way that that guidance can be—the way that that guidance can be realized at the different agencies. And that delta is going to cause people who are individually empowered authorizing officials trying to leverage this AI to make decisions on whether or not it is good or bad based on some of the definitions that could use some more specificity frankly.

So, I am very concerned that it is going to lead to risk-averse views of AI when we right now need to be embracing the technology where——

Ms. MACE. Thank you. I am going to give the last 25 seconds to Ms. Goodloe. Thank you for yielding back.

Ms. GOODLOE. Thank you, Chairwoman Mace. I think the need to coordinate actions across agencies is one of the biggest challenges and opportunities with this executive order.

We see a range of agencies tasked with conducting different reports, consultations, and issuing rules, and I think the need to coordinate those to ensure we have a harmonized policy across agencies is imperative.

One thing the Administration can do is to make sure they are consulting with stakeholders to better coordinate.

Ms. MACE. Thank you.

All right. I will now yield to my colleague, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you so much, and great testimony from all of our panelists.

Dr. Ho, among your six recommendations, you touched on AI officers. To whom should the AI officers in respective agencies report?

Dr. HO. Yes. Thank you for the question, Representative. I think this goes back to what Congresswoman Mace had asked earlier which is, an earlier study of the two prior EOs and how they were implemented within agencies showed that there were some real inconsistencies. And part of that, from our sense, was actual fragmentation within the agency——

Mr. CONNOLLY. So—all right. I have got a limited time, and org charts matter.

Dr. HO. Yes.

Mr. CONNOLLY. Shouldn't the AI officer report to the CIO—primary CIO?

Dr. HO. I think that, actually, in my view, depends on what kind of resources the CIO has available.

Mr. CONNOLLY. OK. Well, when you go back to Stanford, think about it, because this matters. The fragmentation of management over cybersecurity, IT, AI, you know, what could go wrong with that?

When we wrote FITARA, we had 240 people with the title CIO in 24 agencies—250. No private sector company would put up with that, no matter how big.

Dr. HO. Yes. Representative, I agree, and that is why one of our——

Mr. CONNOLLY. All right.

Mr. HO [continuing]. Recommendations early on was to actually ensure that the——

Mr. CONNOLLY. Right.

Dr. HO. [continuing]. Right guy was placed at——

Mr. CONNOLLY. Which is what I picked up on. But I think we have to really nail down, going to Ms. Goodloe's point, we cannot have it, you know, all over the place. There has to be some systemized set of standards and management practices and principles and titles with responsibility—comparable responsibility, because you cannot take that for granted in the Federal Government.

Dr. HO. I agree.

Mr. CONNOLLY. All right.

Ms. Goodloe, you talked about NIST and saying it really should be the foundation for AI management. Let me just ask—and I do not mean anything by this, but a devil's advocate question—is this the right agency? Why not GSA? Why not OMB?

You know, NIST has a very specific mandate, set of responsibilities. It does not make sense to house AI in NIST.

Ms. GOODLOE. This is a very important question, so thank you. NIST's role as an expert agency is a key resource for the Federal Government. NIST's creation of an AI risk management framework is a significant achievement, and it was done at the direction of Congress.

The expertise that has gone into that framework can be leveraged across the government by agencies looking to implement AI risk management practices. And so, we recommend that the NIST framework be the anchor of how agencies use and procure AI systems, so that they manage risk in a coordinated way.

Mr. CONNOLLY. I am agnostic about whether it should or should not. It is in the EO, but I would ask myself—maybe I would ask you this question—do you think NIST has the requisite experience dealing with the private sector?

Because the AI experience is coming out of the private sector, and that means the government has got to intersect with private sector entities. And sometimes that works well, sometimes it does not.

What about the culture at NIST, do you think that is going to work well, intersecting with the private sector? Because making that relationship work is going to be critical.

Ms. GOODLOE. You are right, it is critical, and we do think NIST is the right agency to lead expertise on this. Their work on the AI risk management framework builds on this success in creating risk management framework for things like cybersecurity and for privacy.

The cybersecurity framework has become a gold standard worldwide for governments and organizations looking to manage cyber risks, and we think their expertise has been put to great use in creating the AI RMF.

Mr. CONNOLLY. OK. That is good to hear. I am going to ask two more questions. One is just affirm or not, but in listening to all of your testimony, basically I heard you say—and I am not trying to put words in your mouth—the EO is a good start, got a lot of things right. We are worried about unintended consequences. We are worried about did it go far enough—Mr. Hammond—but at least it is a good start and creates a foundation with which we can work. Is that a fair statement from all of your point of view?

Mr. HAMMOND. Yes, sir.

Dr. HO. Yes.

Dr. CHOWDHURY. Yes.

Mr. CONNOLLY. So, let the record show all of our panelists answered in the affirmative.

OK. My final question, and I hope we have time, what keeps you up at night? What should we worry about with respect to AI? We know the good it can do. What about the other part?

Dr. Chowdhury, why don't you start.

And if the Chair will just give me a little liberty to allow you to answer, I will shut up.

Dr. CHOWDHURY. Well, first and foremost, we have empirical data that there Is bias and discrimination that occurs in AI systems today. This comes from the underlying data.

AI is simply a model or a representation. When it takes action, it is taking action as a representation of the data that has been fed into it and the designs that have happened to it.

So, as we think about implementing AI, AI being built for the public sector needs to work for 100 percent of the people from day 1. This is not a commercial product. This is not an Uber for puppies.

You know, these are things that critically matter to individuals, so we have to be very careful in how we roll things out, so that they are equitable for all. Thank you.

Oh, and to your previous point about NIST, I would just want to add that two of my former team from Twitter are actually currently at NIST, so NIST is certainly a draw for folks in industry.

Ms. MACE. I am so generous, so generous.

Mr. CONNOLLY. You are, you are.

Ms. MACE. I actually want to hear from the rest of the panelists, what keeps you up at night? Ten seconds or less.

Mr. CONNOLLY. Exactly. Thank you, Madam Chairwoman. I am really fascinated with that question.

Mr. HAMMOND. Well, as I talked about in my written statement, progress in AI is accelerating so quickly that now the current forecast for artificial general intelligence, a system that could, in principle, do anything a human could do, or better, are as soon as 2026.

And so, one of the things I worry about is that as we go to NIST and other organizations to set standards, is that these standards will become obsolescent really quickly because it is a moving target.

And second, that if we do not win that race to AGI, that China will. And in addition to my work on this stuff, I always work on things like expert controls——

Ms. MACE. Right.

Mr. HAMMOND [continuing]. And one of the big glaring loopholes is China's ability to access our CHIPS through Cloud services in Singapore and elsewhere. We have to close that loophole.

Ms. MACE. Scary.

Dr. Ho?

Dr. HO. Government cannot govern AI if it does not understand AI. We need the people and information in order to seize this particular moment.

Ms. MACE. Thank you.

Ms. Goodloe?

Ms. GOODLOE. And on that note, we also need the right AI policy. The U.S. needs to be a leading voice in establishing AI policy and be a strong leader worldwide on this issue.

Ms. MACE. Mr. Nodurft?

Mr. NODURFT. I worry about the appropriate government resources available to fund and to work with the people that are in the organizations to train them accordingly so that they can leverage the AI technology.

Ms. MACE. Thank you.

And I will now yield 5 minutes to Mr. Timmons, my colleague from South Carolina.

Mr. TIMMONS. Thank you, Madam Chair. I am actually intrigued, none of you mentioned anything that involved AI-enabled weaponry. I mean, AI-enabled, armed drone swarm would really kind of be the end of the world as far as a terrorist attack goes. I mean, there is all kind of potential uses for it.

Anyways, thank you, Madam Chair. I appreciate you holding this hearing on such an important and timely issue.

As we stand on the precipice of a technological revolution driven by AI, it is imperative that our regulatory frameworks are not only sufficient to manage risk and foster innovation in this emerging technology, but are also harmonized across all of government.

Artificial intelligence has the potential to revolutionize industries, drive economic growth, and enhance the quality of our lives.

However, with great power comes great responsibility. As we witness the rapid advancements in AI technology, it becomes increasingly clear that a patchwork of disjointed regulations is not sufficient to address the complex challenges and ethical considerations that AI presents.

Earlier this year, NIST released its AI risk management framework. The AI RMF will give companies, agencies, and others who utilize AI a common resource when adopting risk management programs.

This will align and coordinate AI risk management across organizations. It is a step in a right direction.

Ms. Goodloe, you mentioned the importance of the NIST RMF in your testimony. What are the benefits of that guidance for both agencies and the private sector?

Ms. GOODLOE. Yes. Thank you for the question. The NIST framework is a significant accomplishment, and one benefit of the NIST framework is, it allows organizations to adopt risk management practices that have the same structure so that they have a common approach to managing AI risks and they have a common language for managing those risks.

In our view, the risk management framework developed by NIST should anchor how agencies use and procure AI systems. When agencies and their vendors adopt risk management practices based on the RMF, they speak the same language, and they can better coordinate and manage risks across entities.

Mr. TIMMONS. Thank you for that.

And how can the OMB's approach to AI be improved through congressional action to assist in the harmonization of the litany of issues you raised in your written testimony?

Ms. GOODLOE. In our view, the OMB memo is a significant achievement in taking a risk-based approach to AI risk management, but it can be improved in several ways, and my written testimony highlights them.

First, there is a need for a governmentwide approach to procurement of AI systems.

Second, there Is a need for a uniform definition of the types of AI systems that are subject to this memo. Right now, the definition of "rights-impacting" and "safety-impacting" are broad enough that you can imagine two different agencies reaching two different conclusions about whether one AI system meets those definitions.

Finally, we think the OMB memo should better leverage NIST's work in creating the risk management framework and look to that further as a resource to drive the U.S. Government's approach to using and procuring AI technologies.

Mr. TIMMONS. Sure. Thank you for that.

And I guess one last question, why is it important for the government to buy commercially available products instead of products specifically made for the government, and how would the EO or OMB memo play into that process?

Ms. GOODLOE. Yes. This is an important point, and I think it needs to be a focus for implementation of the OMB memo. The government should be encouraging agencies to buy commercially available products which are historically subject to less high-failure rates.

They are not likely to go obsolete. They are easier to update and, therefore, less vulnerable to threats, and often less expensive than products that are made specifically for the government.

So, we think both the Administration and the OMB guidance should encourage agencies to buy commercially available products.

Mr. TIMMONS. Sure. Thank you.

Dr. Ho and Mr. Nodurft, one final question. You both touched on this in their question about what keeps you up at night. How can Congress create a regulatory framework that protects against potential harm associated with AI while not impeding the development and implementation of all the benefits that AI has to offer?

And I am going to say that another way. I am concerned that businesses will just relocate abroad if our regulatory framework becomes overly complex or burdensome. So, what can we do to strike the right balance? Dr. Ho?

Dr. HO. Well, I think it is critical that we lead with values. There are values that are embedded in technology, and one of the big questions facing us, do we want—is whether we want a small number of Silicon Valley firms to embed those values, whether we want our foreign adversaries to embed those values, or whether we want broader forms of democratic input to kind of embed those values.

That is why, for instance, in my opening remarks, I support R&D by passing the bipartisan CREATE AI Act to really ensure that small businesses and a wider range of Americans can really participate in the AI revolution.

Mr. TIMMONS. Mr. Nodurft, I will followup in writing. I do not want to take more time.

Mr. NODURFT. Sure.

Mr. TIMMONS. Thank you, Madam Chair. I yield back.

Ms. MACE. You look scared.

OK. I will yield 5 minutes to Mr. Lynch for questions.

Mr. LYNCH. Thank you, Madam Chair.

In its final report, the bipartisan National Security Commission on Artificial Intelligence underscored that the preservation of U.S. leadership in global AI largely depends on our ability to present a democratic model, governing the use of AI for national security to the rest of the world. Dr. Chowdhury, is that even possible? I have my doubts.

Dr. CHOWDHURY. In short, yes. One of my recommendations is for the U.S. to invest in not just top-down leadership but bottom-up, by creating systems, tools, procedures, processes similar to what I just came from back in Singapore, to imbue our democratic values in implementation of AI systems to be made widely available.

Mr. LYNCH. I just see us in a competition, you know, and I know China right now has full spectrum surveillance of its entire population. It has no constraints at all in terms of, you know, respecting individual rights or any—they do not have any internal structural restraints that we do in terms of serving a democracy.

I just wonder if, because of the restraints that we have, the strength of our government itself and our desire in government to make sure that individual rights are respected in this technological process, whether or not we just forfeit too much in terms of allowing China to get very far ahead of us.

That is just not a—there is not a good ending to that story if we allow that to happen.

The other aspect of this that I worry about is the power of AI, and I know it has been around for a while but not like it is now. I mean, we have—you know, Mr. Timmons talked about the weaponization of weapon systems that would be completely autonomous, things like that, that we are trying to struggle with in terms of our military capabilities.

I just, I see a lot more danger there than I think I have heard represented on this panel. And I know government. I have been here over 20 years. And while the velocity of change is incredible in science and technology, we have not changed much up here.

You know, we got rid of the powdered wigs, you know, but that is about it in the last—we still call the cloak room the cloak room, and someone with a cloak has not walked in here in over a hundred years.

So, there is some real limitations in our form of government, our democracy. We have a lot of restraints on us that other governments do not, and I am just very worried that we are going to forfeit any opportunity we have to develop the type of democratic model of AI that others are urging us to create.

And, I do not know, I just—how can we, in the United States, in developing our AI policy, influence other countries, even in Europe, friendly, you know, and allies, other democracies, how do we make that happen?

Dr. CHOWDHURY. You know, as a political scientist, I hear what you are saying as kind of an age-old question, right? Is it easier or simpler to have an authoritarian government that just tells ev-

erybody what to do and enforces it? And it is true. They move incredibly efficiently.

But what we have found time and time again is that they do not last. They end up being cults of personality. They end up being untenable situations. They do not respect the rights of individuals. And at some point, people get fed up with it.

We saw this during World War II and what happened in the cold war, where it turned out that even in the countries that had, you know, presumably mass support from the people, that they actually looked to America. And it seemed silly to think that, you know, blue jeans and rock-and-roll tapes were the things that swayed hearts and minds, but that is what happened.

And I actually think that, in a future where AI is imbued into a lot of processes and a lot of things that we do and influences our daily lives, people will look more toward autonomy. They will look toward a better future.

AI is meant to develop human flourishing. Even the for-profit companies like OpenAI say that they are building AI toward the benefit of humanity. How can we achieve that if it is just controlled by a few individuals?

Mr. LYNCH. Madam Chair, my time has expired. Thank you for your courtesy.

Mr. CONNOLLY. Madam Chair, before you recognize our colleague, I am informed Representative Summer Lee is on her way and would request to be waived on to the Subcommittee. I have no idea when she will arrive.

OK. Thank you.

Ms. MACE. I will now recognize Representative Burlison for 5 minutes.

Mr. BURLISON. Thank you, Madam Chair.

And thank you for everyone that is joining the panel today.

The Biden executive order on AI is over 100 pages long. It includes dozens of new and, I think, far-reaching reforms, guidelines, rules, and programs. It tasks over 50 Federal entities with approximately 150 different requirements.

And while I have done my best to evaluate its scope and impact, I appreciate the Chairwoman for holding this hearing because I think it is helpful to understand the implications of this.

And I will say that, generally speaking, my attitude on innovation and technology should be—is that we should be laissez-faire. We should be hands-off in any approach, especially to such a new and emerging industry.

As I recall through the history of programming—from machine to assembly to procedural programming to general purpose—I mean, all of it was developed not by government establishing rules on the way in which people should be coding or creating some form of outline.

Fortran was invented by IBM—OK—without any input from the Federal Government. BASIC was invented by Microsoft without any guidelines or any rules or anything that was passed by an executive order. SQL—again, by IBM—and then lately, Apple created Swift. All of this has been done by the creative forces in the private sector.

So, my question to the panel—and we will just begin with Mr. Hammond at the beginning—is, do you have any concerns? I mean, everybody on the panel has said that they support this new executive order, but do you understand my concerns about how this might throttle back innovation?

Mr. HAMMOND. Yes, sir. I mean, you know, one of the reasons we are leaders in software is because software has been the exception to the rule of our physical industries. You do not need to get permission to build a new app in the same way you do to build a transmission line or to build a refinery.

And for that reason, it is why we are the leader in AI. And many of the issues that are coming up around deepfakes and so on and so forth, those will get market solutions. You know, no company wants AI users to be flooding their services, they are going to be developing tools, tools that are going to be iterating faster than we can set standards.

Mr. BURLISON. Yes. To me, I think of the days, you know, when computers first came out, and you had viruses that were occurring, and people did not know what to do, and now you have antivirus software to address it. I think you are going to have—you are certainly going to have some things—some nefarious things happen with AI, but the counterpunch to that is, you know, white-hat AI.

Mr. HAMMOND. Right. Spam filters.

The one exception I would draw is, if you look at how the EO talks about these dual-use foundation models, dual-use can be a big term, but the EO is quite narrow in how it defines that to include things that can produce biological agents, cyber weapons, things of that nature, and I think that is a reasonable exception to the rule.

Dr. HO. If I may, it is one of the reasons—your concern is one of the reasons why I express skepticism about a licensing regime that would restrict development of large foundation models to a very small number of actors potentially.

And I think the other thing I want to add here is that, you know, it is true that we have had a thriving innovation ecosystem that we should promote in order to maintain America's leadership in AI.

That said, part of what has been so important has been basic R&D investment by the Federal Government that led to innovation that occurred over the long term, including basic algorithmic research that has powered the AI revolution, but also basic things like radar, the internet, and GPS devices that we each have in our pockets.

And so that is why the parts of the EO that are really investment-oriented, like the National AI Research Resource sponsored in the CREATE AI Act, are so important.

Mr. BURLISON. I think Ms. Goodloe wants to say something.

Ms. GOODLOE. I do. Thank you.

On the executive order, I think it is important to look at its breadth and the number of actions it takes and to recognize that the implementation of those different rules and initiatives will matter. And we will know more about the effects of this executive order as those rules are implemented as we see regulation——

Mr. BURLISON. This sounds a lot like we will find out what is in it after we pass it.

Ms. GOODLOE. We will know more as these initiatives are taking effect and as we see the rules coming down.

But I want to also acknowledge that there are real risks with AI, and a thoughtful United States policy on AI can help increase trust in the technology that is good for the economy broadly.

Mr. BURLISON. All right. Well, don't you think that—I mean, some of the things that might happen are not new to mankind. Theft being used through AI is still theft, right? Violence or hate speech or anything like that, all of that is not new.

Sorry. I am over my time.

Ms. MACE. Thank you.

Great questions of our panelists today.

And in closing, I want to thank everybody. And I want to thank my colleagues on both sides of the aisle for being here this afternoon and having this very important discussion.

You know, we all have a lot of enormous concerns about the advances in AI because it has just gone by so quickly. And I think we have to be very careful about—before we even think about regulating AI, we have to first figure out how our own existing laws today already apply.

You cannot create bioweapons as it is today. Why would AI be any different? AI obviously could not be helpful in that either.

So, I think we have to be very careful and thoughtful so that we do not stifle innovation because we want the United States to lead around the world. We do not want China to catch up with us, and in order for that to happen, we have to keep innovating.

And I think knowing what I know now, as a sophomore 2.5 years in here up on the Hill, is that the Federal Government moves like just the slowest dinosaur. I mean, we are still on mainframe computers and legacy systems, and we should not be. How in the hell do we think we could make advances in AI vis-&-vis the government? I mean, that is just not ever going to happen.

And so, I think we have got to be very careful about it, but it is worth having this discussion on how we try to protect people, consumers, or data in the Federal Government, et cetera. How can we use AI to advance the ball in many ways and take what is going on in the private sector and using it in the public sector?

And I think we are going to have to rely on—significantly rely on the private sector to—what does ethical AI look like? Because they are the ones that are going to have to take the lead.

And I would call on industry today in AI to take the lead. What does that look like? And encourage industry and companies to work together on that framework and what that might look like in the future.

And with that, I will yield to my Ranking Member.

Mr. CONNOLLY. Thank you, Madam Chairwoman. This has been a most illuminating hearing and really thoughtful.

I want to just say to my friend before he leaves, I think he makes a really good point about what could be achieved with sort of unimpeded private sector research.

But I would say to my friend, we have to acknowledge, as Dr. Ho did, that the Federal Government has some stunning successes in its own research and development. We would not have the inter-

net but for what was called DARPANET for 25 years, a 100-percent-funded Federal R&D project.

We would not have mapped the human genome without a 100-percent-federally funded research project, which is going to transform medicine. We would not have GPS, which is now universal but was a classified Department of Defense technology until we decided to open it up commercially. We would not have radar. There is a whole string.

Sometimes the narrative of the Federal Government is really skewed. I do not mean to suggest my friend did that. He was pointing out the positive aspects of private sector unimpeded, and I agree with that. I come from the private sector, too.

But we have to acknowledge the Federal Government has done some spectacular things. The internet. How do you even put—how do you put an ROI on the internet? What has the return on that investment been? I think it is approaching infinity because it has transformed the whole world. It is very hard to put a dollar figure on it, but thank God we made that investment. And I just point that out.

Mr. Hammond talked about the pace. We have to be concerned about the pace because we are in a race not only with the natural evolution of this technology, but with competitors who are accelerating or exploiting that pace.

I listened to a podcast today—I think it was just in the last week—with Elon Musk. And he was asked, well, on the pace and evolution of AI, when do you think we arrive at a point where AI overtakes human intelligence? The smartest brain on the planet, AI can do better. And his answer was within 3 years. Not 30. Three.

So, we do have challenges, and keeping up with that and making sure that we get it right—as you said, Ms. Goodloe, we have got to get it right. We do not want to impede. We do not want to thwart or, you know, suppress, but on the other hand, we want to protect.

And we want to try to anticipate how we channel AI into purposeful and positive, you know, betterment for the quality of human life while protecting humans from the worst it could produce, and getting that right is going to be a big challenge. And as the Chairwoman said, we are going to need the private sector as a partner as we proceed to do this.

Thank you so much for being here, and thank you, Madam Chairwoman, for this hearing.

Ms. MACE. Yes.

And I see that our colleague has arrived, so I will ask unanimous consent for Representative Summer Lee from Pennsylvania to be waived on to the Subcommittee for today's hearing for the purposes of asking questions.

Without objection, so ordered.

Ms. Lee, I will recognize you for 5 minutes of questioning.

Ms. LEE. Thank you, Madam Chair, and to the Committee for allowing me to waive on. And thank you so much for your patience for extending, Madam Chair and Ranking Member Connolly, and to all of our experts for sharing your testimony today and for the important work addressing this issue.

It is good to see you again, Dr. Chowdhury. Of course, I have seen you on the SST Committee.

The President's October 2023 executive order on AI acknowledges that, to appreciate the benefits of AI technology, we have to first mitigate substantial risk it poses of perpetuating existing biases. The individuals who are most marginalized in our community, such as those with disabilities, are left most vulnerable to these risks.

In my district, an Associated Press investigation found that the family risk predictor tool used by a child protective services agency harbored potential bias against people with disabilities. The civil rights repercussions of these opaque AI tools, or black boxes, are alarming, and those impacted are left with little to no options for recourse.

So, we must approach AI development and implementation with ample caution to ensure that the technology serves everyone equitably. For this to happen, diversity and inclusion must be fundamental at every stage of AI development process.

Dr. Chowdhury, how can we ensure that diversity and inclusion ultimately influence the outcomes of AI systems?

Dr. CHOWDHURY. Thank you for the question. It is great to see you again as well.

Well, first, we have to start with diverse teams. And I could not help but notice that, of the agencies that have named chief AI officers, only the NSF has a woman at the lead. And this matters. This matters in industry. This matters in government as well. I encourage the government to seek diverse candidates to set direction and perspective.

Second, there must be checks for diverse data. In engineering, we have this phrase, "garbage in, garbage out." AI is simply a reflection of the data and the design decisions that have been made to create the system.

Overwhelmingly, we see AI systems reflect the biases that exist in society. For example, there was a kidney allocation algorithm that discriminated against Black patients because of a history of systemic discrimination by doctors.

And finally, there needs to be testing—such as red teaming—for minority perspectives when relevant for the use of the product. For example, facial recognition that does not recognize different skin tones.

Ms. LEE. Yes. Thank you.

The AI executive order highlights the importance of increased investment in AI research and education, such as what has taken place at Carnegie Mellon University in my district.

Since the 1950's, CMU has been at the forefront of AI development and recently announced a collaboration between their Responsible AI initiative and NIST to host a workshop with the goal of operationalizing the NIST AI Risk Management Framework. AI auditing and assessment is an integral element of building equitable systems.

Dr. Chowdhury, as CEO and cofounder of Humane Intelligence, a nonprofit that provides AI assessments for clients, what are some of the major barriers you have observed in translating ethical AI principles to practice?

Dr. CHOWDHURY. The primary barrier of adopting AI in general is reliability and consistency. So, while those of us in tech are impressed with compute size and speed, the biggest companies in the world—those who provide tangible solutions for consumers—are interested in good customer experience. So, it is not a good customer experience if an AI model hallucinates, discriminates, impacts mental health, and so on.

Companies are actually looking for sensible boundaries and not barriers to adopting AI. I use the phrase, "brakes help you drive faster." So, one of the implementation or adoption of responsible AI is the requirement to create tools and systems that integrate into how a company builds and deploys AI systems.

I have done this for about 7 years at this point. It is certainly possible. But we need to think about operationalization, measurement, and what sort of rules and standards can be interoperable and universal.

Ms. LEE. At this point, there is a lot of hype surrounding AI, and it' has become hard to separate fact from fiction. There is a concern that exists among the public about AI existentialism, a fear experienced by many that AI will someday become fully autonomous or even sentient.

Dr. Chowdhury, if you could cut through the AI hype for us, are these concerns about artificial general intelligence and AI existentialism well-founded?

Dr. CHOWDHURY. In short, no. What our well-founded concerns are the already established discriminatory practices introduced by unmonitored AI systems in surveillance, criminal justice, healthcare, financial services, education, and more.

Ms. LEE. Thank you.

Just to close, we have to continue to uphold the priorities of safe, secure, and trustworthy AI to guarantee that everyone can reap the benefits of the technology. In upholding these priorities, it is crucial that we continue to bring attention to the AI harms that are disproportionately impacting marginalized communities, as you have laid out for us today.

I thank you all so much for being with us today and for your testimony, and I thank you so much for the time today.

Thank you. I yield back.

Ms. MACE. Thank you.

And my colleague from Tennessee just showed up. So, we saved the best for last.

Mr. Burchett, you have 5 minutes.

Mr. BURCHETT. Thank you, Chairlady. And thank you for bringing this to the forefront.

I am still not exactly sure what this is all about or what you all do, but I am learning.

So, as I sit up here, you have got a bunch of old guys that are still in powder-blue leisure suits with zingo-dingo zip-up boots and are still listening to 8-tracks in their 1972 AMC Gremlin fastback. So, I mean, that is who you are calling on to regulate this, and I am kind of afraid of the regulation because we could end up stifling something that could be really good for this country and this world.

Mr. CONNOLLY. Can I say to my friend, I think you are speaking for yourself. The only thing I even knew what you just said was eight-track.

Mr. BURCHETT. And I loaned him my Johnny Paycheck eigth-track, and it is the Christmas special. I will be needing to get that back here pretty soon. Thank you, sir, as always.

Dr. Ho, do you know of any instances of foreign countries like China who are using artificial intelligence to oppress its citizens?

Dr. HO. There are indeed foreign adversaries who have used AI to repress populations. And to step back here a little bit, all of this is happening in the context of this kind of geopolitical competition where China, for instance, has announced that it wants to be the world's leader in AI by 2030.

Just to go back to your opening remarks, though, I think you are right to sort of express the concern about overregulating. And that is why, in my opening remarks, the thing I am quite, sort of, fond of is a kind of adverse event reporting system, where for cybersecurity harms, harms of medical devices, there are ways to drive down the information gap of what is known in the private sector and between government so that we can have forms of regulation that are not overbearing and that are actually tailored to the kinds of harms that have manifested.

Mr. BURCHETT. Let me ask you—do not punch your button yet, Dr. Ho—does China use this to advance its agenda abroad, and if so, how?

Dr. HO. Yes. As we have seen in other instances with, you know, hardware like the ones involving the company Huawei, there are real concerns about our foreign adversaries using technology as a way to influence countries. That is why I think international collaboration around these issues is going to be central.

It is really good to see that, in the EO, we are seeing, you know, an entire section dedicated to really fostering multilateral collaboration amongst like-minded countries so that we can have a form of tech diplomacy so that the values that are encoded in these kinds of systems are ones that are really representing the kind of American values that exist here.

For instance, you have—related to some of the earlier discussion of the NIST AI RMF, the executive order requires a development playbook of how to actually adapt the RMF framework to work with other countries, and there are also proposals, like the Multilateral AI Research Institute, to try to bring like-minded countries together.

That was a recommendation endorsed by the National AI Advisory Committee on which I sit, to actually bring like-minded countries together to formulate a collaborative approach to AI governance.

Mr. BURCHETT. What about Executive Order 14110? Do you think it goes far enough to allow us to compete against China?

Dr. HO. I think the executive order, as I said in my opening remarks, is a really important first step. It is the first step, and I think there are numerous other steps that I think—I am hoping Congress will take, particularly to invest in leadership within government, to bring talent both to the government—to have a pipe-

line of folks within agencies, but also to train, retain, and attract talent here to the United States.

Maybe one fact I can give is that 40 percent of engineering and science Ph.Ds. in the country are visa holders, and historically, we, as a country, have been remarkable at retaining that talent. One estimate has it that 80 to 90 percent of those Ph.Ds. stay in the country.

Recently, there have been signs that that has been changing, and we do not, at this point, want a kind of brain drain where people are leaving the country. And I think the EO's provisions that are particularly speaking to the immigration front on that side, I think, are quite important.

We, as a country, have to remain a magnet for scientific talent for us to retain the kind of leadership position that we currently enjoy.

Mr. BURCHETT. All right.

Yes, sir.

Mr. HAMMOND. Just to your question about China and the way they use AI, a few months ago, my former colleague Geoffrey Cain testified in the Senate about his book "The Perfect Police State," which discusses China's use of AI to monitor the Uyghur population as a pilot program for their country as a whole.

And I think, as AI disrupts institutions worldwide, there is going to be a race among every tin-pot dictator out there to import technology to restore security, and one of the roles the U.S. can play is by developing defensive technology that can do things like policing and law enforcement while preserving civil liberties.

Mr. BURCHETT. All right. I have run over my time.

Ranking Member, Chairlady, it has been wonderful. Thank you so much.

Ms. MACE. Thank you.

And with that, and without objection, all Members will have 5 legislative days within which to submit materials and to submit additional written questions for the witnesses, which will be forwarded to the witnesses for their response.

If there is no further business, without objection, the Subcommittee stands adjourned.

[Whereupon, at 3:26 p.m., the Subcommittee was adjourned.]