

# HOW ARE FEDERAL AGENCIES HARNESSING ARTIFICIAL INTELLIGENCE?

---

---

## 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

SEPTEMBER 14, 2023

**Serial No. 118-64**

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

53-382 PDF

WASHINGTON : 2024

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio	JAMIE RASKIN, Maryland, <i>Ranking Minority Member</i>
MIKE TURNER, Ohio	ELEANOR HOLMES NORTON, District of Columbia
PAUL GOSAR, Arizona	STEPHEN F. LYNCH, Massachusetts
VIRGINIA FOXX, North Carolina	GERALD E. CONNOLLY, Virginia
GLENN GROTHMAN, Wisconsin	RAJA KRISHNAMOORTHY, Illinois
GARY PALMER, Alabama	RO KHANNA, California
CLAY HIGGINS, Louisiana	KWEISI MFUME, Maryland
PETE SESSIONS, Texas	ALEXANDRIA OCASIO-CORTEZ, New York
ANDY BIGGS, Arizona	KATIE PORTER, California
NANCY MACE, South Carolina	CORI BUSH, Missouri
JAKE LATURNER, Kansas	JIMMY GOMEZ, California
PAT FALLON, Texas	SHONTEL BROWN, Ohio
BYRON DONALDS, Florida	MELANIE STANSBURY, New Mexico
KELLY ARMSTRONG, North Dakota	ROBERT GARCIA, California
SCOTT PERRY, Pennsylvania	MAXWELL FROST, Florida
WILLIAM TIMMONS, South Carolina	SUMMER LEE, Pennsylvania
TIM BURCHETT, Tennessee	GREG CASAR, Texas
MARJORIE TAYLOR GREENE, Georgia	JASMINE CROCKETT, Texas
LISA McCLAIN, Michigan	DAN GOLDMAN, New York
LAUREN BOEBERT, Colorado	JARED MOSKOWITZ, Florida
RUSSELL FRY, South Carolina	<i>Vacancy</i>
ANNA PAULINA LUNA, Florida	
CHUCK EDWARDS, North Carolina	
NICK LANGWORTHY, New York	
ERIC BURLISON, Missouri	

MARK MARIN, Staff Director

JESSICA DONLON, Deputy Staff Director and General Counsel

RAJ BHARWANI, Senior Professional Staff Member

LAUREN LOMBARDO, Senior Policy Analyst

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	GERALD E. CONNOLLY, Virginia <i>Ranking Minority Member</i>
TIM BURCHETT, Tennessee	RO KHANNA, California
MARJORIE TAYLOR GREENE, Georgia	STEPHEN F. LYNCH, Massachusetts
ANNA PAULINA LUNA, Florida	KWEISI MFUME, Maryland
CHUCK EDWARDS, North Carolina	JIMMY GOMEZ, California
NICK LANGWORTHY, New York	JARED MOSKOWITZ, Florida
ERIC BURLISON, Missouri	<i>Vacancy</i>
<i>Vacancy</i>	

C O N T E N T S

---

Hearing held on September 14, 2023 .....	Page 1
--	-----------

WITNESSES

---

Dr. Arati Prabhakar, Director, White House Office of Science and Technology Policy Oral Statement .....	5
Dr. Craig Martell, Chief Digital and AI Officer, Department of Defense Oral Statement .....	7
Mr. Eric Hysen, Chief Information Officer, Department of Homeland Security Oral Statement .....	9

*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

---

- \* Questions for the Record: to Dr. Martell; submitted by Rep. Connolly.
  - \* Questions for the Record: to Dr. Prabhakar; submitted by Rep. Mace.
  - \* Questions for the Record: to Dr. Prabhakar; submitted by Rep. Connolly.
- Documents are available at: docs.house.gov.*



# HOW ARE FEDERAL AGENCIES HARNESSING ARTIFICIAL INTELLIGENCE?

Thursday, September 14, 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 1:02 p.m., in room 2247, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Timmons, Burchett, Edwards, Langworthy, Burlison, Connolly, Lynch, Khanna, and Mfume.

Also present: Representative Higgins.

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

Without objection, the Chair may declare a recess at any time.

And I would like to say that Ranking Member Connolly is just running a few minutes late, but we have another Member here. We are going to go ahead and get started, give everybody plenty of time, and they will be rolling in momentarily.

I would like to recognize myself for the purpose of making an opening statement.

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

At the very first hearing of this Subcommittee held earlier this year, expert witnesses told us artificial intelligence, or AI, is likely to bring disruptive innovation to many fields. AI should instigate economic growth, higher standards of living, and improved medical outcomes.

Virtually every industry and institution will feel the impact of AI. Today, we will discuss the impact of AI on the largest, most powerful institution in the Nation: the Federal Government.

As we know, the government today performs an ever-expanding swath of activities, from securing the homeland, to predicting the weather, to cutting benefits checks. Many of these functions could be greatly impacted by AI. That is clear from the hundreds of current and potential AI use cases posted publicly by Federal agencies

pursuant to an executive order issued under the last administration.

Federal agencies are attempting to use AI systems to enhance border security, to make air travel safer, and to speed up eligibility determinations for Social Security disability benefits, just to name a few cases.

AI will also shake up the Federal workforce itself. We hear a lot about how AI could disrupt the private sector workforce, transforming or eliminating some jobs while creating others. While the Federal Government is the Nation's largest employer, and many of those employees work in white collar occupations, AI is already reshaping because it can perform many routine tasks more efficiently than humans. That will allow Federal employees to focus on higher order work that maximizes their productivity.

In fact, a Deloitte study estimated the use of AI to automate tasks of Federal employees could eventually yield as much as \$41 billion in annual savings by reducing required labor hours. A separate study by the Partnership for Public Service and the IBM Center for The Business of Government identified 130,000 Federal employee positions whose work would likely be impacted by AI, including 20,000 IRS tax examiners and agents. That, of course, begs the question whether we need to hire tens of thousands of new IRS employees when AI could transform even or replace the work of much of its current staff. I think every American could agree with that.

AI can make government work better, but it is still just a tool, be it an incredibly powerful one, and like any tool, can easily be abused when used for the wrong purposes or without the proper guardrails.

AI systems are often fueled by massive troves of training data that flow through complex algorithms. These algorithms can yield results, and their own designers are unable to predict and struggle to explain sometimes, and we are learning this in real time.

So, it is important we have safeguards to prevent the Federal Government from exercising inappropriate bias. We also need to ensure the Federal Government's use of AI does not intrude on the privacy rights of its own citizens. The bottom line is we need the government to harness AI to improve its operations while safeguarding against potential hazards.

That is why Congress enacted the AI in Government Act in late December 2020, soon before the current Administration took office. That law requires the Office of Management and Budget to issue guidance to agencies on the acquisition and use of AI systems. It also tasked the Office of Personnel Management with assessing Federal AI workforce needs. But the Administration is way overdue in complying with the law.

OMB is now more than 2 years behind schedule on issuing guidance to agencies, and OPM is more than a year overdue in determining how many Federal employees have AI skills and how many need to be hired or trained up.

I will also say, in the Administration's cybersecurity plan before it was made public, I asked the question pointedly to the Administration if AI was even included in it at the time, and it was not.

It is mentioned three times fleetingly, very casually in that document today.

The Administration's failure to comply with these statutory mandates was called out in a lengthy white paper issued by Stanford University AI Institute. The paper authors also found that many agencies had not posted the required AI use case inventories. Others had omitted key use cases, including DHS submitting an important facial recognition program.

The Stanford paper summed up the Administration's noncompliance with various mandates by concluding: America's AI innovation ecosystem is threatened by weak and inconsistent implementation of these legal requirements.

Most of the AI policy debate is focused on how the Federal Government should police the use of AI by the private sector, but the executive branch cannot lose focus from getting its own house in order. It needs to appropriately manage its own use of AI systems consistent with the law.

This Subcommittee will keep insisting the Administration carry out laws designed to safeguard government use of AI, and I am developing further legislation to ensure Federal agencies employ AI systems effectively, safely, and transparently. We have a huge opportunity before us, and I would love to see us harness the technology that is rapidly evolving. I expect this hearing will help inform many of these efforts.

Ms. MACE. And with that, we are going to go to—we are going to go to our witnesses, and when Ranking Member Connolly comes in, we will give him time for his opening statement.

I am pleased to introduce our witnesses for today's hearing. Our first witness is Dr. Arati Prabhakar, Director of the White House Office of Science and Technology Policy and Assistant to the President for Science and Technology, earning her the designation as the President's science advisor. Dr. Prabhakar is also the first science advisor to be nominated to the President's Cabinet.

This is Dr. Prabhakar's first appearance as a witness before Congress since her Senate confirmation last year.

We are pleased to have you here today. I am grateful that you showed up. I will tell you not everybody does, and they sometimes send the under secretary of the under secretary or the assistant to the assistant to the assistant. And it is refreshing to have someone actually show up that we have asked for, and I just want to thank you for your time today.

Our second witness is Dr. Craig Martell, Chief Digital and AI Officer with the Department of Defense. And our third witness is Mr. Eric Hysen, Chief Information Officer with the Department of Homeland Security.

We welcome everyone. We are pleased to have all of you here this afternoon.

So, pursuant to Committee Rule 9(g), the witnesses will, please, if you will stand, and raise your right hand.

Do you solemnly swear or affirm the testimony 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.

So, we appreciate all of you being here today and look forward to hearing your testimony.

I would like to 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. As a reminder, please press the button on your microphone in front of you so that it is on, and Members 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. And when the red light comes on, your 5 minutes has expired, and we would ask that you just please wrap it up for us.

All right. So, with that, I am going to yield to our Ranking Member of the Subcommittee, Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chairwoman.

I have got three subcommittee hearings today and two caucus meetings, so I am a little bit out of breath, but thank you. Thank you for accommodating me.

Earlier this week, Majority Leader Chuck Schumer held his inaugural AI insight forum and Senator Hickenlooper held a hearing on the need for transparency in artificial intelligence.

Today, our Subcommittee returns for a second hearing on AI to discuss its uses within our own Federal Government. I think it is very clear all Members of Congress are interested. I am not sure it is clear how much Members of Congress know about it.

This Subcommittee is proud to continue its historical leadership in the AI space. As many of you know, former Subcommittee Chair, Will Hurd, held a three-part hearing series on artificial intelligence, and the late former Chairman, Elijah Cummings, focused primarily on facial recognition.

These initiatives show that, if done right, the Federal Government can leverage AI to better serve the public. For example, several Federal agencies are already using AI technologies to cut costs, improve constituent services, and strengthen existing systems. The United States Cyber Command and the Department of Homeland Security, for example, employ AI technology to protect our networks in counter-cyber attacks.

The United States Postal Service is currently piloting an autonomous vehicle project that employs AI technology. The Department of Housing and Urban Development and the U.S. Citizen and Immigration Services are using AI chatbots to facilitate communication with the public looking for help from the agency.

However, like all new tools, if used improperly, AI could result in unintended consequences. For example, automated systems can inadvertently perpetuate societal biases, such as faulty facial recognition technology or opaque sentencing algorithms used by our criminal justice system. AI can also threaten jobs, proliferate misinformation, and raise serious privacy concerns.

That is why I applaud the Biden Administration for proactively taking significant steps to ensure transparency in the government's use of AI.

Last October, the White House released a blueprint for an AI Bill of Rights to ensure the protection of civil rights in the algorithmic age. Prior to that, the National Artificial Intelligence Initiative Act



codified the establishment of the American AI Initiative and the National AI Advisory Committee.

This Subcommittee looks forward to hearing an update from the panelists before us on the joint work with the Secretary of Commerce to advise the White House on that AI policy.

Everybody can agree the government has a colossal responsibility in developing the necessary guardrails to curb the risk of this incredible technology while allowing it to flourish. This Committee must hold Federal agencies accountable to ensure that they are making appropriate choices about whether and when AI is right for their mission.

The Federal Government must also intentionally train, recruit, and maintain a workforce that is comfortable and confident with this technology. That is why the Chairwoman and I worked to pass the AI Training Expansion Act of 2023, H.R. 4503, out of our Committee and would expand AI training within the executive branch. Really important. And I commend my colleague for that bipartisan collaboration.

AI is already changing the world around us in so many ways, and we need to step up to the challenge and mitigate the risks. The Federal Government needs to ensure this technology is created, deployed, and used in a safe, ethical, productive, and equitable manner.

And with that, I yield back. Thank you, Madam Chairwoman.

Ms. MACE. Thank you, Mr. Connolly.

I ask unanimous consent for Representative Clay Higgins from Louisiana to be waived on to the Subcommittee for today's hearing for the purpose of asking questions.

So, without objection, so ordered.

I would now like to recognize Dr. Prabhakar to please begin your opening statement.

**STATEMENT OF DR. ARATI PRABHAKAR  
DIRECTOR  
WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY  
POLICY**

Ms. PRABHAKAR. Thank you so much, Chairwoman Mace. And thanks to you, Ranking Member Connolly, Members of the Subcommittee. I have really appreciated the work that you all are doing on artificial intelligence, and it is great to be here with my colleagues to be able to spend this time to focus on these important issues.

I have three messages today, and the first one is that AI is a top priority for President Biden. He is very clear that this is one of the most powerful technologies of our times. When we look around the world, we can see that every Nation is racing to use AI to build a future that is imbued with their own values, and I think we can all agree that we do not want to live in a future that is defined by technology shaped by authoritarian regimes. And that is why the President is very clear that American leadership in the world today requires American leadership in artificial intelligence.

Second, for America to lead in AI, government has some core responsibilities, and one of those, one set of those responsibilities is to manage the risks of AI. And as both of your opening statements

have noted, AI's risks are broad because its applications are so broad, and these risks range from risks related to fraud and information integrity. They include risks related to safety and security, risks associated with privacy, civil rights, civil liberties, and risks to jobs and the economy.

Now, some of these risks can be addressed under existing laws and regulations. Some of these risks can be managed by making sure that government uses AI responsibly, and in some cases, we do expect that legislation will be required. That is about mitigating risks.

The reason we are doing all of this work to manage risks is so that our country can seize this technology to build the future. And if you look at what companies are doing, they are racing to build better products and services to transform industries using AI, and this is a technology that holds equally great promise for the work that government does for the American people. And that then becomes a second core responsibility of government.

I think both of you have spoken to that as well in your opening remarks.

You are going to hear from my colleagues about national security and homeland security, and there is a lot to be said there. I will also just briefly touch on the many other important services and the public purposes that are government's responsibility. And when you look across Federal Government today, you will see that agencies are starting to use the insights that they can glean from these vast troves of data that they generate in the doing of their business.

AI technology is also changing the way government agencies interact with their citizens. They can speed it up. It can simplify it. It can just make those administrative processes work much better. The examples are very wide-ranging. They include AI for weather prediction. They include AI to help us keep air travel safer. AI is being used to speed up the processing of disability determinations. It is being used to improve how we process patent applications, and those are just an example today.

If you take a peek inside of labs around the country and look at what is happening with federally funded R&D, in the world of research and development you will get a glimpse of where the future is going, and AI is playing a huge role there as well because AI can enable the design of the materials that we need for advanced batteries, for hydrogen storage, the things that are critical to our clean energy future.

AI can change the way that we predict disasters, the way that we implement plans for resilience as the climate changes. AI can transform drug design. It can allow us to tailor clinical care to each individual patient's needs. It can enable major advances in population health.

Used responsibly, AI can help us deliver better outcomes and to create new possibilities for the American people.

My third message for you, and I will end with this, is that the Biden-Harris Administration is taking action to meet this moment. We have moved with urgency on a series of steps that started with the AI Bill of Rights that we published almost a year ago, and I want to emphasize that, especially in a time when technology is

moving as fast as it is, it is so important to be clear about our values, about the importance of rights, about safety and security, about privacy. And that was the important role of the AI Bill of Rights.

More recently, because of the President's leadership, 15 companies have now made voluntary commitments to focus on safety, security, and trustworthiness in their AI systems that they are developing and driving. That is companies' responsibilities.

Today, the White House is working—

Ms. MACE. We are running out of time. I apologize. We are going to be voting soon, so if you can—

Ms. PRABHAKAR. I will wrap up.

Ms. MACE. Yes.

Ms. PRABHAKAR. Absolutely.

Ms. MACE. Thank you.

Ms. PRABHAKAR. We are working today in the White House on an executive order. The Office of Management and Budget is working on guidance for departments and agencies. That is the executive branch. We continue to work with our international allies because AI does not stop at the borders. And finally, we remain committed to working closely with Congress on a bipartisan basis as you consider legislation.

I will just finish by saying this work is urgent, it is important, and I very much look forward to working with you on it.

Ms. MACE. Thank you.

And I will recognize Dr. Martell to please begin your opening statement.

**STATEMENT OF DR. CRAIG MARTELL  
CHIEF DIGITAL AND AI OFFICER  
DEPARTMENT OF DEFENSE**

Mr. MARTELL. Chairwoman Mace, Ranking Member Connolly, and distinguished Members of the Subcommittee, thank you very much for inviting us here today.

And I would like to start just by asking the question, what is AI? And so, we should have a sort of common definition in our head as we are going through this. So, when I say the phrase "artificial intelligence," I simply mean statistics at scale.

We gather massive amounts of data from the past. We use it to build a model, and we use it to predict the future. It is really important to think about it that way because it is statistics at scale, which means it is never 100 percent correct, which means for every model that we build, it will always, sometimes, get it wrong. And so, a large part of what we have to think about is how do we understand when it gets it wrong, and what should we do when it does get it wrong. So, it is really important to rethat as I am going through my comments. My other panelists here may have different definitions, but that is the operative one for me.

I look forward to sharing the ongoing efforts of the Chief Digital and AI Office around the responsible use of data analytics and AI-enabled technologies to accomplish our national defense mission.

Data analytics and AI are integral to accomplishing the priorities set forth in the National Defense Strategy. To support these efforts, the CDAO has established five strategic initiatives: Improving data

quality; that is the stuff we use to measure the past. Developing robust performance metrics; that tells us how well we are doing in the future. Providing enterprise-ready AI scaffolding; building the data integration layer for CJADC2; and developing a robust talent management plan for the Department of Defense as a whole.

First, quality data is CDAO's foundational priority. We are focused on holistically improving the quality of the data that enables most DOD use cases. For example, CDAO is providing data and digital talent teams to the principal staff assistants and the combatant commanders through the Accelerating Data and AI Initiative, also called ADA.

Additionally, the CDAO is creating validation and verification processes that check data for errors, inconsistency and, with respect to bias, class imbalances, before AI models are ever even produced. We are also working closely with the U.S. Cyber Command on their 5-year AI roadmap for rapidly acquiring and adopting AI systems.

Second, in business performance, CDAO, in partnership with the DOD performance improvement officer, is defining and data-enabling the metrics that the DOD will use to assess and manage its performance in support of the Secretary of Defense's priorities, the National Defense Strategy, and the strategic management plan. CDAO is ensuring that these metrics are outcome-based, not just how many meetings did I go to, but the effectiveness of those meetings, and measurable.

Third, enterprise AI scaffolding consists of the robust environments and tools that enable cutting-edge development of machine learning and AI capabilities. We provide the technical and nontechnical enterprise services necessary to accelerate secure, reliable, and responsible AI development.

Fourth, for CJADC2, CDAO is focused on building the data integration layer that will enable data-centric command and control across the Department and with our partners and allies. CDAO is iteratively assessing the necessary capabilities for this data integration layer via a series of experiments called GIDE, Global Information Dominance Experiments. And these experiments are in their seventh iteration and currently underway now. GIDE 8 is scheduled for December, and I am happy to brief the Committee on the successes that we have been having in GIDE.

Finally, in order to enable data-driven capabilities across the entire Department of Defense, we are building a unified digital workforce program with the chief talent management officer and other under secretaries. The goal of this program is to develop a digital workforce that is globally identifiable and readily accessible for DOD use.

Ladies and gentlemen, within all of these initiatives, I want to clarify that AI is not a singular, monolithic technology, nor a one-size-fits-all solution. That is extremely important. When we say AI, it is not something that if we have it, we win, and if they have it, we lose.

We need different algorithms, different success criteria, and different data to train the different models underpinning each of our different use cases. Think about the different use cases in your daily lives: talking to your phone, getting shopping suggestions,

does this shirt go with those pants, and using a search engine to find the information you need. Each of these require very different AI technologies.

The same is true for the DOD. We need computer vision to understand our environment; natural language processing to navigate the Department's policies and idiomatic language, which is really hard for humans to understand; and reinforcement learning for predictive maintenance; as well as many other types of machine learning algorithms.

It is very important to remember that AI is neither a panacea nor a Pandora's box, and if we think about it that way, we are not thinking about it correctly and we are not going to be able to tackle the problem. It is not a one size thing. We need to evaluate its effectiveness and concomitant dangers on a use case by use case basis.

Ms. MACE. We have got to wrap it up. I apologize.

Mr. MARTELL. I am done. That was my last word.

Ms. MACE. Great, thank you. There you go. Awesome. Bravo.

I would like to recognize Mr. Hysen to please begin your opening statement.

**STATEMENT OF MR. ERIC HYSEN  
CHIEF INFORMATION OFFICER  
DEPARTMENT OF HOMELAND SECURITY**

Mr. HYSEN. Chairwoman Mace, Ranking Member Connolly, and distinguished Members of the Subcommittee, thank you for the opportunity to testify today.

I would like to note that in addition to serving as the Department's Chief Information Officer, Secretary Mayorkas also named me today as the first DHS Chief Artificial Intelligence Officer.

I would like to talk with you today about three concrete use cases where DHS is already using AI to deliver clear benefits for the American people and then share the comprehensive measures we are taking to ensure that our use of AI is safe, responsible, and rights respecting.

First, DHS is using AI to keep dangerous drugs out of our country. Recently, a car drove north from Mexico and approached the San Ysidro port of entry in San Diego, California. In the past, the Customs and Border Protection officer that inspected that car would likely have had no reason to give it extra scrutiny. But this time, one of our machine learning models noticed a potentially suspicious pattern in the vehicle's crossing history. After looking at the model's flag, the officer decided to refer the car to secondary inspection, where we discovered and seized nearly 60 kilograms of fentanyl and 16 kilograms of meth concealed in the vehicle's rear quarter panels and gas tank. If not for this use of AI, those drugs could be on our streets.

Second, DHS is using AI to aid our law enforcement officers in investigating heinous crimes. Last month, Homeland Security Investigations announced the completion of one of the most successful operations ever against child sexual abuse online.

Operation Renewed Hope resulted in identifying 311 previously unknown victims of sexual exploitation and led to the rescue of several victims from active abuse and the arrests of suspected per-

petrators. This operation relied on the expertise and dedication of our agents and our partners domestically and abroad, but our agents had an extra tool at their disposal.

Machine learning algorithms were used to enhance older images and give investigators new leads. Through this use of AI, we were able to turn formerly cold cases into rescues and arrests.

Finally, DHS is using AI to make air travel easier and safer. TSA has started rolling out touchless pre-check in select airports, a new optional way of going through the airport, curb to gate, without ever taking out your wallet. Once you opt in, you can check your bag, go through the security checkpoint, and board your flight all with just a quick photo.

This process and TSA's acceptance of mobile driver's licenses in seven states, and counting, used thoroughly tested AI powered algorithms to save time, reduce physical touch points, and increase security by verifying identity more accurately.

While I have highlighted these three examples today, DHS will use AI to transform all parts of our operation, from detecting and mitigating cybersecurity vulnerabilities to enhancing maritime search and rescue operations and far beyond. AI will provide smarter and timelier information to our agents and officers to aid them in making decisions and free them up from routine tasks to focus on higher value work.

As we move forward, we will ensure that our use of AI is responsible and trustworthy; that it is rigorously tested to be effective; that it safeguards privacy, civil rights, and civil liberties, while avoiding inappropriate biases; and to the extent possible, that it is transparent and explainable to the people we serve.

Last month, Secretary Mayorkas issued our key principles for responsible AI use. We are applying these principles through the DHS AI Task Force, which I lead alongside our Under Secretary for Science and Technology, by issuing comprehensive policies on specific types of AI, as we did just this week with new restrictions on our use of facial recognition.

We will work alongside our internal and external oversight partners, to include Congress and this Subcommittee, as we work to implement NIST's AI risk management framework and remain fully compliant with evolving laws, practices, and policies.

Thank you again for the opportunity to testify today. I look forward to your questions.

Ms. MACE. Thank you, Mr. Hysen.

I know votes have just been called. I am going to, before I gavel out—and my colleagues can leave to go vote. I am just going to ask my questions before we go and gavel out.

Dr. Prabhakar—I am going to recognize myself for 5 minutes.

My first question is to you, Dr. Prabhakar. As the President's science advisor, you are the President's top artificial intelligence advisor, I expect you regularly brief him on AI. The Associated Press has quoted you as saying in a recent interview you have had several conversations with him about AI.

How many times have you been able to brief him thus far in this position?

Ms. PRABHAKAR. Thank you for the question, Chairwoman. The President has been very focused on AI. He has asked for briefings on AI at multiple junctures.

Ms. MACE. How many times have you been able to brief him?

Ms. PRABHAKAR. I would have to stop and count. Let me give you a couple of examples. He met——

Ms. MACE. Is it more than one?

Ms. PRABHAKAR. Multiple times. He met with his council of advisors, PCAST, and the President's Council of Advisors on Science and Technology. I believe that was in early April. We had a discussion about AI before that, and then he spent an extended period with a room full of amazing science and technology experts, people using AI, people generating AI, and had a very extensive conversation there.

Another occasion was——

Ms. MACE. What did President Biden say to you about AI?

Ms. PRABHAKAR. President Biden has spoken publicly many times about AI and——

Ms. MACE. What has he said to you in these conversations about AI?

Ms. PRABHAKAR. Obviously, I am not in a position to say what he said in the Oval. I will tell you what he has said publicly, which is very consistent, which is he recognizes how fast it is moving, how it is part of this pivot point in history, and the choices that we make are essential. He is very excited about the potential——

Ms. MACE. How would you characterize his level of understanding of AI? Do you think he understands?

Ms. PRABHAKAR. I think it is excellent. The questions—he grills me, and he grills everyone else who——

Ms. MACE. He grills you?

Ms. PRABHAKAR. Yes.

Ms. MACE. What does he grill you on?

Ms. PRABHAKAR. Well, I can talk about the things that he has said publicly, and they are on many topics. He has talked about the ways that AI can be used. He has expressed concerns about the way that it can create problems. He has talked about the fact that he is married to a schoolteacher, and so he knows about how it shows up in education.

Ms. MACE. Does he understand its uses within the Federal Government? That is sort of outside, I mean, education. I mean, in the Federal agencies and how it can be utilized, does he understand that? Does he talk about anything relevant to the progressive AI?

Ms. PRABHAKAR. The President is very clear about the breadth of applications of artificial intelligence, and his vast understanding, of course, is many years as a legislator and now as——

Ms. MACE. Vast.

Ms. PRABHAKAR. President, of all the functions of government, of the role that it plays in national security, but also in all the other functions of government. He understands, obviously, that it is clearly going to be powerful.

Ms. MACE. The Office of Science and Technology Policy is not a regulatory agency. It is a White House policy shop. So, can you explain what role you and your office play with respect to Federal AI policy? How does that work?

Ms. PRABHAKAR. We have several roles. And as OSTP, a core role is to be the place where the Federal R&D enterprise comes together, where we work together and make sure that people know what each other are doing in areas across research and technology but including information technology and artificial intelligence.

When a massive new shift like this great acceleration in AI happens, one of our important roles is to be clear with our colleagues in the White House, with the President, with our colleagues in departments and agencies about how the technology is progressing, what issues they will need to contend with, what the big opportunities are.

And that means that in the case of AI, our National AI Initiative Office, which Congress established at OSTP a couple years ago, that cadre of people in my organization have been extraordinarily busy mapping out the risks, the opportunities, and informing policy—

Ms. MACE. So, a question about some of that. What are some of the operations of your office? It maintains governmentwide AI use case inventory. Is that correct?

Ms. PRABHAKAR. Working with the Office of Management and Budget.

Ms. MACE. That inventory has been appropriately criticized in the press as being inconsistent and incomplete. The inventory is lacking uniformity, and some significant AI use cases have been omitted.

So, is your office doing anything to improve the inventories, to improve transparency with the public? What does that look like?

Ms. PRABHAKAR. The initiative to start cataloging those use cases was an important one, and it is very much work in progress. We are getting good insights from what is already in that use case inventory and working with departments and agencies—

Ms. MACE. And then one last question. I have got 25 seconds.

OMB is more than 2 years late in complying with a congressional mandate to give Federal agencies guidance on the acquisition and use of AI. The law requires OMB to coordinate with your office in drafting that guidance.

So why—and very quickly. We have 10 seconds. Why is the process stalled? When can we expect to see some guidance?

Ms. PRABHAKAR. The Office of Management and Budget is working in a very focused manner on what they clearly understand—

Ms. MACE. Two years late.

Ms. PRABHAKAR.[continuing] is a priority.

Ms. MACE. Thank you so much.

Ms. PRABHAKAR. We will get there.

Ms. MACE. Our time is up, and I yield back.

And pursuant to the previous order—and I apologize because we are out for votes—the Chair declares the Committee in recess, subject to the call of the Chair. We will stand in recess for votes.

Thank you.

Mr. EDWARDS.

[Presiding.] Welcome back, everyone. Pursuant to the previous order, the Chair declares the Committee in recess—OK. Let us start that over.

The Committee will come back to order.



And the Chair recognizes Representative Langworthy for 5 minutes.

Mr. LANGWORTHY. Thank you, Mr. Chairman.

I would like to thank all of our witnesses for being here today to continue driving the artificial intelligence conversation forward. The opportunity that the Federal Government has to implement AI into its everyday operations is potentially exciting for the future of the country and for the modern workforce.

However, I would like this Subcommittee, and all of us, to consider the impact of AI and other emerging technologies on our younger generation. While AI has numerous benefits that I am sure will be discussed here today, it has serious implications on our youth, especially when it comes to generative images and child exploitation. I would be more than happy to work with Chairwoman Mace and the rest of our Oversight Committee to address these concerns.

But before we do that, I want to speak about some of the AI frameworks that have been developed. Specifically, the National Institute of Standards and Technology has a well-established track record of developing frameworks and recommendations to improve cybersecurity outcomes in the Federal Government. Earlier this year, NIST published a groundbreaking AI risk management framework, which was developed at Congress' direction in an open multistakeholder process.

Leading companies are already using the NIST AI framework for managing AI risks, just as they use the NIST cybersecurity framework and other NIST cyber recommendations.

With that being said, Dr. Prabhakar, I would like to ask you whether or not you see the NIST AI framework being taken up by the Federal Government in the same way that NIST cybersecurity work is being used today, and what steps, if any, that your office is taking to implement the AI framework?

Ms. PRABHAKAR. Thank you so much, Representative Langworthy. NIST—I had the great pleasure of leading NIST many decades ago when my hair was still black, and I share your important point about the role that that organization has played in cybersecurity and other important areas. In artificial intelligence, their risk management framework, when they put that out, I think that was one important step in a longer journey to getting to where we can actually have safe and effective AI, whether it is private sector use or public sector use.

And as you have seen with industries' adoption of the risk management framework and its—I see that approach also starting now to be used within government. What that allows people to do is to know what questions to ask about how to make an AI system safe and effective. And again, depending on the application, the questions will be different and the process that they go through will be different. But that is a starting point. And to me it is just table stakes to know that, you know, if your organization is using that risk management framework, it is table stakes to know that you are actually asking the question.

I want to step back, though, and also be clear that what we all are—we all understand that what we need is a future where AI systems are safe and effective, that they do what you need them

to do, that they do not do dangerous things or inappropriate things that you do not want them to do. But I think we should all be very clear that companies, researchers, nobody actually really quite knows how to do that.

And so, I think NIST's work and the technology community's work that is still ahead is to continue to develop tools and methods so that we can get as good at understanding whether an AI system is safe and effective as we know for physical products in many other areas, and that is some of the work that still remains to be done.

Mr. LANGWORTHY. I wanted to follow up and ask about criticism toward the AI blueprint that OSTP has produced, the blueprint that has been criticized for being in conflict with the NIST framework. Could you address this?

Ms. PRABHAKAR. I would be happy to address this. The AI Bill of Rights focused on our values, which are so important when we are in very choppy times and choppy waters as this technology is moving so fast. And if you go back and look at the Bill of Rights, what it talks about is how important it is to make sure that people have—are not discriminated against but have access to safe systems that are secure.

So, a lot of the same themes that you will find in the risk management framework and everything that we have been talking about here today, that is very consistent with the Bill of Rights. That work was developed by OSTP but working very closely with NIST and others across government with many, many inputs from private organizations, companies, civil society organizations, academics.

And then when NIST built the risk management framework on the heels of that, again, there was a lot of close communication and coordination. And to me it was—part one was values of the Bill of Rights. Part two was the initial steps of how does an organization start grappling with what are the processes that they need to put in place to manage these risks.

Mr. LANGWORTHY. Unfortunately, I am out of time, and I yield back, but we will be following up with some questions in writing.

Ms. PRABHAKAR. I look forward to it.

Mr. EDWARDS. The gentleman from New York yields, but I would like to yield my 5 minutes back to Mr. Langworthy.

Mr. LANGWORTHY. Well, thank you very much.

I also wanted to bring up an executive order issued by the last administration requiring Federal agencies to post for public view most of their AI use cases. This is intended to give the public a view into the Administration's current and planned use of AI systems. But many of these agency inventories are missing or they are incomplete, according to a Stanford University AI Institute whitepaper which was issued last December.

Do you agree that the public has a right to know for what purposes AI is being used by the Federal agencies and that it is important that these inventories are done consistently, completely, and accurately? And will you pledge to work to continue to ensure that that is the case?

Ms. PRABHAKAR. Thank you very much, Mr. Langworthy, for that question.

I share your focus on the value of those use cases for all the reasons that you mentioned. It is important for the public to know and across government for people to understand how AI is being used, and there is important progress that we are making and will continue to make as a Federal Government on those AI use cases.

Thank you.

Mr. LANGWORTHY. Transparency I think is something that we all need to fight for, especially as this emerging technology is coming at us so quickly.

I want to see if regulatory sandboxes have been part of your conversations. The European Parliament approved its AI Act, which includes a conversation about setting up coordinated AI regulatory sandboxes to foster innovation in artificial intelligence across the EU.

Do you see regulatory sandboxes having success in the EU and whether or not do you think they will be successful in the United States?

Ms. PRABHAKAR. My colleagues may have answers on that, Mr. Langworthy. I do not think I have enough information to give you a complete answer. I will just note that we continue to work with our colleagues and allies in Europe and around the world simply because AI is happening everywhere, and different regions are taking somewhat different approaches. But we are finding that with our like-minded allies, we all share this focus on getting to a safe and effective AI future, and I think there will be some important collaborations that are possible there.

I do not know if others have other comments on that topic.

Mr. MARTELL. So, we think being able to work effectively with AI with our partners and allies is extremely important. So, we have been focusing a lot, not only on the data sharing and how do we do that effectively according to regulations, but also how do we build models together and evaluate the effectiveness of those models together. And so, we have a number of initiatives working through that.

Mr. LANGWORTHY. Mr. Hysen?

Mr. HYSEN. No, nothing to add on regulatory approaches. We defer to the White House.

Thank you.

Mr. LANGWORTHY. OK. With the remaining time, I want to focus on the Department of Homeland Security. So, Mr. Hysen, are you concerned that as AI systems become more mature and complicated, that criminals will have greater opportunity to commit heinous crimes, like child exploitation?

Mr. HYSEN. Congressman, we absolutely are concerned there; however, we are also looking to harness AI to combat those crimes. I shared earlier our work of Homeland Security Investigations in Operation Renewed Hope, which used AI to help rescue victims from active abuse, as well as to arrest suspected perpetrators. So, as we are looking to better defend against the use of AI to commit these crimes, we are also using it to defend against them.

Mr. LANGWORTHY. The protections, you know, have to be built at the same time as, you know, all of the fruits of what AI can bring us. They have to be there. Our most vulnerable, I believe, are those most likely to be harmed by, you know, a lot of this AI technology.

Now, I will expand the scope of this question and include America's adversaries unleashing increasingly powerful cyber-attacks against U.S. critical systems. What is DHS doing in preparation to respond with the use of AI in those respects?

Mr. HYSEN. Absolutely. We are, and have been for the entire Administration, concerned about adversarial use of AI against Federal and critical infrastructure networks. Secretary Mayorkas established our Artificial Intelligence Task Force, which I co-lead, and charged us with looking at the use of AI to secure critical infrastructure as one of our critical objectives. We are working with the Cybersecurity and Infrastructure Security Agency to look at how we can effectively partner with critical infrastructure organizations on safeguarding their uses of AI and strengthening their cybersecurity practices writ large to defend against evolving threats.

Mr. LANGWORTHY. Very good.

I yield back, Mr. Chairman.

Mr. EDWARDS. The gentleman yields.

Next, the Chair recognizes the Honorable Mr. Khanna from California for 5 minutes.

Mr. KHANNA. Thank you, Mr. Chair.

Dr. Martell, I thought your description of AI as statistics on scale was one of the best I have heard. Was that your phrase or is that someone else's?

Mr. MARTELL. You know, these things get bounced around. I think it is mine, but it might not be, so I do not want to claim anything that is not, but it is one I have been using for a while for explanatory purposes.

Mr. KHANNA. Well, I appreciate it, because I think—you know, I do not always agree with Noam Chomsky, but I thought his op-ed in the New York Times where he talked about human intelligence and what that entails and how that is so different than a predictive model that is taking a lot of data and putting probabilistic outcomes was very thoughtful.

And one of the concerns I have is that there is been an overhyping of AI as a form of human intelligence, which I just think is giving our species less credit than we deserve. So, I appreciated your clarification.

Dr. Prabhakar, Chairwoman Nancy Mace and I have a bill called the SEARCH Act, which would basically require government agencies to use AI technology to help improve the search functions in their own websites in collecting data. Could you help describe what the benefits of having AI do that kind of search for government agencies could be?

Ms. PRABHAKAR. Representative Khanna, thank you for your leadership on that matter, as well as other issues related to AI.

And I think you have described it very clearly. If you step back and you think about how much the government does that is about interacting with citizens, providing information, taking information, those are areas where this new generation of language-based AI, of course, can have tremendous benefits, but it has to be used thoughtfully and carefully.

And search is a great example. It is easy to imagine the use—and people are starting to do this—using generative AI to summarize complex documents, to synthesize arguments from across many

different perspectives, to draft responses. And I emphasize draft because as anyone who has worked with these technologies knows, I think what we are seeing, private sector and public sector I think are finding that there are few cases we are simply relying on a chatbot will solve a problem, but there are many cases where that interaction might be the beginning of accelerating a workflow or improving the way that you do whatever you do.

So, I think those are interesting examples, and they are different and distinct and build on top of the many ways that government agencies are using AI on sensor data or data that they collect that is not language-based. So, I think this is this next chapter that is starting to unfold, and I appreciate your focus on it.

Mr. KHANNA. I appreciate that.

And, Dr. Prabhakar, when you look at AI—and obviously these things are hard to predict—how do you think over the next 10 years it will have an impact on jobs? Is it a case of augmenting people's talent?

I have often said to Hollywood, my concern is not that if they had AI bots write all the scripts, that it is not able—that they would not be able to do it. My concern is it will just be terrible. You know, they are not going to produce Hamlet. It will just be the further devolution of entertainment.

Many a times I have used ChatGPT, and I have challenged my staff to use it for a speech, and it is not as good as Cliff's Notes. And if professors are having students use it and not getting good grades, it is probably because they are not asking the right questions. I mean, probably the class is not challenging enough.

But my point is that, where is it that it is going to displace things? How do we prepare for it? Where is it that it is going to create opportunity as you see it?

Ms. PRABHAKAR. This focus on the impact of AI technology on jobs is critically important because we have a long history. We know that technology does change work in all kinds of ways. And it is, I think—let me just start by saying that it is very early, and right now we do not fully know. It has not fully played out how this new generation of language-based AI will—how will it blossom and what impacts will it have.

The best understanding that many experts have in this area is that there are things that will look a lot like prior changes with technology coming in, and there are things that are not going to look the same.

What I think we can expect is that some jobs may get upskilled, become more valuable, allow people to earn more for their labor, and other jobs will get displaced. That has happened with every wave of technology for not just decades but probably for millennia.

And I think what is very different about this new generation, of course, is the fact that it can be used to do administrative tasks, creative tasks, everything from graphic design and image generation to writing documents to even legal analysis, and so a lot of the kinds of professions that a few years ago I think people imagined were not going to be touched by AI technology now will come into the limelight.

Mr. KHANNA. My time has expired. I am still waiting for ChatGPT to come up with something as eloquent as statistics with scale, but we will see.

Ms. PRABHAKAR. That is right.

Mr. MARTELL. I do not think that is possible, sorry.

Mr. EDWARDS. And so, with that, the Chair now recognizes the Honorable Representative Timmons from South Carolina for 5 minutes.

Mr. TIMMONS. Thank you, Mr. Chairman.

Thank you to all our witnesses for being here.

Dr. Martell, I want to start out with you. You defined AI in a way that I have never heard before and in a way that is not really what other searches would define it as. Can you elaborate on that definition?

Mr. MARTELL. Sure. So, it actually does not define all of AI. It defines modern AI. There is a lot of prior generational AI that is actually rule-based, expert systems where they have written a bunch of if-then statements. I would not call that statistics at scale.

But modern AI is—all of modern AI—it is based on gathering massive amounts of data from the past. That is our lens into the world. And particularly, it is highly curated labeled data, which represents the task at hand. It is using that to build a model.

And you can just think back to any simple class you had where you did linear regression. That linear regression is the model, and so it builds the model and then it uses that model to predict the future. And I do not think anybody in the scientific community would disagree with that as a general characterization of how modern AI applies.

Mr. TIMMONS. I appreciate you elaborating. I see where you are—I see your point and I agree. I mean, I had not thought of it that way.

Can we talk about possible uses of AI within either DOD or our adversaries' military capabilities?

Mr. MARTELL. Sure. One of the reasons—if I may, one of the reasons I describe it like that is to have people realize that AI is not monolithic. So, when we say AI, what we really mean is a specific AI-based technology or a specific statistically based technology. And it is important to differentiate that, because we may be doing really well for one use case and very poorly in another, and that may be so for our adversaries as well.

And so, if we focus mostly on AI as a monolithic thing, if we have it, we win; if they have it, we lose, then we are actually missing where we should be aiming our attention at: particular capabilities that we want to deliver or capabilities that we want to defend against. And so, we spend a lot of our energy characterizing those.

That is a conversation I am happy to have with you in a different venue.

But there is lots of use cases within the business aspect of the Department of Defense. Doing analysis of the documents with modern, language-based artificial intelligence is really effective. Understanding the environment using computer vision is really helpful. But in that case, when you think about understanding a document or an image being analyzed and some action being taken from that

analyzed image, it is really important to remember that that was a statistical answer.

So, let us say that we say that there is something in that image, right. We are looking for a truck or a school bus, and we say it is a truck, but it is actually a school bus. And the system got it wrong. Called it a truck when it is a school bus. It is really important to us to build systems that are not simply dependent upon that algorithm but that have humans wrapped around it. It is really human machine teaming so that a human can say, oh, no, it got it wrong. And then there is a—because remember, they are statistical, so they will—it will always be the case that every model will sometimes get it wrong. Always be the case that every model will sometimes get it wrong. So, you need to have a human machine teaming structure so that that human can correct the system and feed back the system and make the system better.

Mr. TIMMONS. And I think as it relates to weaponizing it, one of the benefits is the speed at which it can act. And if you have a drone swarm that is AI enabled, I mean, how do you incorporate the human component? Because the whole benefit of using AI in that scenario would be the speed at which it is able to act.

Mr. MARTELL. Correct. I think that is an excellent question and thank you for it, Congressman Timmons.

One thing the military does well is train with technology. And so, you can think about the way our training works over and over and over and over and over again as a way for you to develop justified confidence in a tool, right? If you have justified confidence in your weapon, sometimes it is going to jam, but you still get a sense of the likelihood or the conditions under which it might, and you learn how to use it.

Mr. TIMMONS. I see where you are going. Planning for the training component to make sure that you have answered the question 4,000 times before it is actually done with live fire is the solution.

Mr. MARTELL. That is right. And sometimes it will get it wrong, and then whomever made the decision to deploy that system will be responsible, as we always are. There is always a responsible agent making a decision to deploy a system.

Mr. TIMMONS. And I guess there is—what is concerning is that while our military will likely make sure that there is a human component and a training component, a nonstate actor that does not care about collateral damage—

Mr. MARTELL. Correct.

Mr. TIMMONS [continuing]. And/or consequences of their actions may be able to use the same technology without regard to the necessary collateral damage.

Mr. MARTELL. That is 100 percent correct. And then we see that as a particular use case that we should train against. What are the tools and countermeasures we need for that situation? That is why I think it is really important to not think about it as monolithic but as use case by use case based.

Mr. TIMMONS. Sure. Thank you. Thank you all for being here.

I yield back, Mr. Chairman.

Mr. EDWARDS. The gentleman yields.

Next, the Chair recognizes the Honorable Representative Higgins from Louisiana for 5 minutes.

Mr. HIGGINS. Thank you, Mr. Chairman. I appreciate the Subcommittee waiving me on for me to address this topic.

Ladies and gentlemen, thank you for being here.

Dr. Prabhakar, that is a lovely name, and we appreciate you being here.

Madam, in your opening, in your statement, in your written statement, you say that—one of your quotes, I believe, says AI advances also bring a risk of a deepening erosion of privacy as surveillance increases and as more and more sensitive information is used to train AI systems. You point out that authoritarian governments are already using AI to censor and repress expression and abuse human rights.

Is that part of your statement, ma'am?

Ms. PRABHAKAR. Yes, sir, it is.

Mr. HIGGINS. OK. I am just clarifying.

I have a broader concern I would like to focus on in my limited time here regarding government's use of AI in the enforcement of laws and regulations, and I think I am strongly against that. And I am going to ask you, Mr. Hysen, regarding law enforcement. That is my background. You may not know. But I appreciate the work that has done on the ground at the enforcement level, and I have my concerns there.

But for you, Doctor, you referenced the authoritarian government's use of AI. Talk to us about criminal enterprise or state-sponsored cyber threat enterprise and how that would relate to AI. For instance, like malware AI or Trojan horse AI. We have all—we have seen major compromises of cyber systems at the government level and in the private sector.

In my state of Louisiana, all driver's licenses—if you have a driver's license in Louisiana, your data was compromised. That is pretty much everybody. So, we have stories like this across the country, it affects us all. Seems to me that AI is a tremendous threat in that arena.

Can you address that?

Ms. PRABHAKAR. Thank you for the question, Congressman Higgins. You are focusing on some of the important issues about the power of AI and the—which makes it very appealing to solve hard problems but then comes with these risks that you have highlighted.

Many threads in some of your comments. Let me focus for a moment on the cybersecurity element, because I think it is a great example of the bright and the dark side of AI technology.

What we are seeing with the advances in AI is the ability to write software code more quickly, more securely, more robustly. Those are some of the bright-side advantages. And at the same time, this is a technology that can be used for cyber-attacks to generate—to look for vulnerabilities, to generate attacks more efficiently.

And so, I think that is the landscape. And then the choices that all of our work focuses on, of course, is how do we mitigate those risks and secure it. For example, securing our systems—our cybersecurity systems as well as we can.

Mr. HIGGINS. In the interest of time, you are aware—and your team and the executive branch and the President is aware, we



hope—we have to be very focused on the balance moving forward between the power of AI and the potential dangers of AI.

And I think, primarily, we have to establish security against weaponized AI from criminal networks and from nation-states that will use AI against our Nation. And at the same time, we have to make sure that we do not build AI into our own governmental enforcement systems that would threaten the individual rights and freedoms of Americans.

Mr. Hysen, briefly, you mentioned that AI recognized patterns in the crossing at the border. How would that relate to the instinct—you believe that AI could dull the human instincts and judgment in law enforcement operations similar to the way that—like, many engineers now cannot use a slide rule. We do not remember phone numbers anymore. They are in our contact data. Most Americans cannot read maps and operate a compass anymore. We use GPS. Kids in school cannot—they are not taught cursive script. And yet all our historical documents are written in cursive script.

Do you understand where I am going with this? Please, briefly, if the Chairman will allow, address that as it relates to the instincts of law enforcement.

Mr. EDWARDS. The witness may answer the question.

Mr. HYSEN. Congressman, thank you. I certainly acknowledge the risk and want to assure you that we are leveraging AI as decision support for our law enforcement officers, but that ultimately, our officers are the ones responsible for making law enforcement decisions.

I also see tremendous potential to use AI to remove repetitive paperwork and administrative tasks that our officers have to do that they would tell you, and they would tell me, dulls their focus from their security mission.

Mr. HIGGINS. Thank you, sir. That is the answer I was hoping for.

Mr. Chairman, I appreciate the indulgence. I yield.

Mr. EDWARDS. The gentleman yields.

The Chair would like to thank the witnesses for your time this afternoon.

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

Without objection, the Subcommittee stands adjourned.

[Whereupon, at 2:41 p.m., the Subcommittee was adjourned.]