ADVANCING INNOVATION (AI): HARNESSING ARTIFICIAL INTELLIGENCE TO DEFEND AND SECURE THE HOMELAND

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MAY 22, 2024

Serial No. 118–67

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
58–784 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

Mark E. Green, MD, Tennessee, *Chairman*

Michael T. McCaul, Texas
Clay Higgins, Louisiana
Michael Guest, Mississippi
Dan Bishop, North Carolina
Carlos A. Gimenez, Florida
August Pfluger, Texas
Andrew R. Garbarino, New York
Marjorie Taylor Greene, Georgia
Tony Gonzales, Texas
Nick LaLota, New York
Mike Ezell, Mississippi
Anthony D'Esposito, New York
Laurel M. Lee, Florida
Morgan Luttrell, Texas
Dale W. Strong, Alabama
Josh Brecheen, Oklahoma
Elijah Crane, Arizona

Bennie G. Thompson, Mississippi, *Ranking Member*
Sheila Jackson Lee, Texas
Eric Swalwell, California
J. Luis Correa, California
Troy A. Carter, Louisiana
Shri Thanedar, Michigan
Seth Magaziner, Rhode Island
Glenn Ivey, Maryland
Daniel S. Goldman, New York
Robert Garcia, California
Delia C. Ramirez, Illinois
Robert Menendez, New Jersey
Thomas R. Suozzi, New York
Timothy M. Kennedy, New York
Yvette D. Clarke, New York

Stephen Siao, *Staff Director*
Hope Goins, *Minority Staff Director*
Sean Corcoran, *Chief Clerk*

CONTENTS

Page

STATEMENTS

WITNESSES

FOR THE RECORD

APPENDIX

ADVANCING INNOVATION (AI): HARNESSING ARTIFICIAL INTELLIGENCE TO DEFEND AND SECURE THE HOMELAND

Wednesday, May 22, 2024

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to notice, at 10:07 a.m., in room 310, Cannon House Office Building, Hon. Mark E. Green [Chairman of the committee] presiding.

Present: Representatives Green, Higgins, Guest, Bishop, Pfluger, Garbarino, Ezell, D'Esposito, Lee, Brecheen, Crane, Thompson, Swalwell, Carter, Thanedar, Ivey, Goldman, Garcia, Menendez, Suozzi, Kennedy, and Clarke.

Chairman GREEN. The Committee on Homeland Security will come to order. Without objection, the Chair may declare the committee in recess at any point.

The purpose of this hearing is to receive testimony from private-sector stakeholders relating to the opportunities and challenges presented by the emergence of artificial intelligence and discuss how the Department of Homeland Security can develop and implement certain AI technologies in support of the homeland security mission. I now recognize myself for an opening statement.

In this era of rapidly-advancing technology, I am especially proud to live in a nation of innovators, some of whom join us today. Today, American ingenuity is paving the way once again. Artificial intelligence or AI promises to transform the global economy and national security landscape as we know it.

AI has the potential to create new jobs, catalyze productivity in Americans' daily lives, and, of course, protect our men and women in uniform and law enforcement.

Throughout this Congress committees in both chambers have convened numerous hearings to understand the countless opportunities and challenges AI presents. Like cybersecurity, AI's impact is a complex and cross-cutting issue that cannot be handled by one jurisdiction alone.

Therefore, we are here to examine what I believe to be one of the most promising areas in which to expand our use of AI, the security and defense of our homeland.

The Committee on Homeland Security has an oversight obligation to make sure we harness AI technologies right. As with any new technology, AI presents new risks and we must take the time to understand them. This includes prioritizing safety and security throughout AI development, deployment, and use.

It also requires us to treat AI with appropriate nuance so that we understand the impact of proposed regulatory measures on our businesses.

Today's full committee hearing follows up on a productive Cybersecurity and Infrastructure Protection Subcommittee hearing led by Chairman Garbarino last December. The subcommittee specifically considered the role of DHS and CISA in securing AI, a topic we will continue to explore today.

As that hearing reaffirmed, the threats facing our country are increasingly complex and DHS plays a critical role in keeping Americans safe and our country secure.

DHS has a broad mission and has explored and even implemented AI for specific purposes aligned with its unique mission. For example, U.S. Customs and Border Protection has used AI-powered systems to monitor border areas using drones and cameras which help identify suspicious activity and unauthorized crossings in real time.

The Transportation Security Administration is currently examining the ways in which AI can enhance its security screening, including using AI to augment its X-ray imaging of travelers' carry-on luggage. TSA may soon look to AI algorithms and particularly facial recognition powered by AI to identify security threats among the traveling public and enhance the prescreening process.

While these AI-powered systems offer the promise of increased security and efficiency, they also bring significant risks that Congress must carefully assess. For instance, AI-powered facial recognition systems capture and store images of Americans and foreign travelers which present substantial privacy concerns. We must ensure that the use of AI-powered facial recognition by TSA is balanced with strong protections of privacy, civil liberties, and ethical standards.

Furthermore, U.S. Immigrations and Customs Enforcement is using AI to help identify and track illegal activities, such as human trafficking and smuggling, by analyzing large data sets and detecting patterns.

The Cybersecurity and Infrastructure Security Agency, CISA, is carefully examining the risks and opportunities presented by AI and the way it can be leveraged to enhance our Nation's resilience against cyber threats. In the years ahead CISA will play a critical role in addressing and managing risks at the nexus of AI, cybersecurity, and critical infrastructure.

Considering the wide-spread push for AI adoption within DHS it is critical that the Department collaborates with Congress and with relevant stakeholders, including those from the private sector, to manage AI's complexities and risks.

In addition to the domestic concerns relating to the emergence of AI, we must also consider the broader strategic implications. Our Nation's primary strategic adversary, the People's Republic of China, has made AI development a national priority and is investing heavily in its research, talent, and infrastructure. The communist regime's aggressive pursuit of AI poses a significant challenge to the United States, not only economically, but also in terms of our national security.

In fact, DHS's 2024 homeland threat assessment warns that developing "malicious cyber actors have begun testing the capabilities of AI-developed malware and AI-assisted software development technologies that have the potential to enable larger-scale, faster, efficient, and more invasive cyber attacks against targets, including pipelines, railways, and other U.S. critical infrastructure." This is extremely concerning.

As complex as these threats are, our Nation's efforts to combat them will be even more challenging if our adversaries lead in AI research, development, and innovation. For these reasons it is important for Congress, DHS, and the private sector to work together to ensure that we remain at the forefront of AI innovation while safeguarding our national security, economic competitiveness, and civil liberties.

Today we will hear from a panel of experts who will provide insights into the current state of AI for homeland security and the steps that we can take to trust that AI, the AI we use will be secure.

To our witnesses, thank you for being here today, for your efforts to educate Members of this committee and the American people on how we can responsibly advance AI innovation. I look forward to your testimony.

[The statement of Chairman Green follows:]

STATEMENT OF CHAIRMAN MARK E. GREEN, MD

MAY 22, 2024

In this era of rapid technological advancement, I'm especially proud to live in a nation of innovators—some of whom join us today.

Today, American ingenuity is paving the way once again. Artificial intelligence, or AI, promises to transform the global economy and national security landscape as we know it. AI has the potential to create new jobs, catalyze productivity in Americans' daily lives, and protect our men and women in uniform and law enforcement.

Throughout this Congress, committees in both chambers have convened numerous hearings to understand the countless opportunities and challenges AI presents. Like cybersecurity, AI's impact is a complex and cross-cutting issue that cannot be handled by one jurisdiction alone. Therefore, we are here to examine what I believe to be one of the most promising areas in which to expand our use of AI: the security and defense of our homeland.

The Committee on Homeland Security has an oversight obligation to make sure we harness AI technologies right. As with any new technology, AI presents new risks, and we must take the time to understand them. This includes prioritizing safety and security throughout AI development, deployment, and use. It also requires us to treat AI with appropriate nuance so that we understand the impact of proposed regulatory measures on our businesses.

Today's full committee hearing follows up on a productive Cybersecurity and Infrastructure Protection Subcommittee hearing led by Chairman Garbarino last December. The subcommittee specifically considered the role of DHS and CISA in securing AI—a topic we will continue to explore today. As that hearing reaffirmed, the threats facing our country are increasingly complex, and DHS plays a critical role in keeping Americans safe and our country secure.

DHS has a broad mission and has explored and even implemented AI for specific purposes aligned with its unique missions.

For example, U.S. Customs and Border Protection (CBP) has used AI-powered systems to monitor border areas using drones and cameras, which help identify suspicious activity and unauthorized crossings in real time. The Transportation Security Administration (TSA) is currently examining the ways in which AI can enhance its security screening processes, including using AI to augment its X-ray imaging of travelers' carry-on luggage.

TSA may soon look to AI algorithms, and particularly facial recognition systems powered by AI, to identify security threats among the traveling public and enhance the pre-screening process.

While these AI-powered systems offer the promise of increased security and efficiency, they also bring significant risks that Congress must carefully assess. For instance, AI-powered facial recognition systems capture and store images of Americans and foreign travelers, which present substantial privacy concerns. We must ensure that the use of AI-powered facial recognition by TSA is balanced with strong protections of privacy, civil liberties, and ethical standards.

Furthermore, U.S. Immigration and Customs Enforcement (ICE) is using AI to help identify and track illegal activities, such as human trafficking and smuggling, by analyzing large datasets and detecting patterns. And the Cybersecurity and Infrastructure Security Agency (CISA) is carefully examining the risks and opportunities presented by AI and the ways it can be leveraged to enhance our Nation's resilience against cyber threats. In the years ahead, CISA will play a critical role in addressing and managing risks at the nexus of AI, cybersecurity, and critical infrastructure.

Considering the wide-spread push for AI adoption within DHS, it is critical that the Department collaborates with Congress and with relevant stakeholders, including those from the private sector, to manage AI's complexities and risks.

In addition to the domestic concerns relating to the emergence of AI, we must also consider the broader strategic implications. Our Nation's primary strategic adversary, the People's Republic of China (PRC), has made AI development a national priority and is investing heavily in research, talent, and infrastructure. The Communist regime's aggressive pursuit of AI poses a significant challenge to the United States, not only economically but also in terms of our national security.

In fact, DHS's 2024 Homeland Threat Assessment warns that developing "[m]alicious cyber actors have begun testing the capabilities of AI-developed malware and AI-assisted software development—technologies that have the potential to enable larger-scale, faster, efficient, and more evasive cyber attacks—against targets, including pipelines, railways, and other U.S. critical infrastructure."

This is extremely concerning. As complex as these threats are, our Nation's efforts to combat them will be even more challenging if our adversaries lead in AI research, development, and innovation. For these reasons, it is important for Congress, DHS, and the private sector to work together to ensure that we remain at the forefront of AI innovation while safeguarding our national security, economic competitiveness, and civil liberties.

Today, we will hear from a panel of experts who will provide insights into the current state of AI for homeland security, and the steps we can take to trust that the AI we use is secure.

To our witnesses, thank you for being here and for your efforts to educate Members of this committee and the American people on how we can responsibly advance AI innovation. I look forward to your testimony.

Chairman GREEN. I now recognize the Ranking Member, the gentleman from Mississippi, Mr. Thompson, for his opening statement.

Mr. THOMPSON. Thank you very much, Mr. Chairman.

Good morning to our witnesses. I would like to thank you for holding this important hearing on the intersection of artificial intelligence and homeland security.

Artificial intelligence is not new. The Department of Homeland Security and its components have a long history of trying to understand how to most appropriately leverage the capacity AI provides. The release of ChatGPT in November 2022 made clear AI's transformative potential, and it accelerated efforts by the administration and Congress to ensure the United States continue to lead the world on the responsible development and the use of AI.

As we consider how to deploy AI to better secure the homeland, we must keep 3 critical principles in mind. First, we must ensure that AI models we use and the data to train them do not reinforce existing biases. That requires that AI used by the Government be developed pursuant to specific policies designed to eliminate bias and is tested and retested to ensure it is not having that effect.

Eliminating bias from AI also requires a diverse AI work force comprised of people from a variety of backgrounds who can identify potential biases and prevent biases from being encoded into the models.

Second, the Government must rigorously assess appropriate use cases for AI and ensure that the deployment of AI will not jeopardize the civil rights, civil liberties, or privacies of the public. Law enforcement and national security agencies in particular must implement an exacting review of potential infringements on those fundamental democratic principles.

Moreover, it is essential that the work force be included in decision-making processes on how AI will be deployed. The work force is in the best position to understand capability gaps and where AI can be affected.

AI is also a tool the work force will use to carry out their jobs more effectively. It is not and should not ever be a replacement for people.

Finally, the AI tools we use must be secured. In many respects, existing cybersecurity principles can be adopted to secure AI. I commend the Cybersecurity and Infrastructure Security Agency, commonly called CISA, for working with the private sector to ensure the adoption of secure-by-design principles in the development of AI.

Moving forward, we must determine vulnerabilities unique to AI and work together to address them. I commend President Biden on last year's Executive Order on AI which put the Federal Government on the path of developing and deploying AI in a manner consistent with these principles.

As DHS continues to assess how it will use AI to carry out its vast mission set from cybersecurity to disaster response to aviation security, I am confident that it will do so in a manner that incorporates feedback from the work force and protect civil rights, civil liberties, and privacy. We cannot allow our optimism about the benefits of AI to short-circuit how we evaluate this new technology. At the end of the day, bad technology is bad for security.

As we consider the potential benefits AI presents for DHS's mission, we must also consider the new threats if proposed. AI in the hands of our adversaries can jeopardize the security of Federal and critical infrastructure networks, as well as the integrity of our elections. We know that China, Russia, and Iran have spent the past 4 years honing their abilities to influence our elections, sow discord among the American public, and undermine confidence in our election results.

Advances in AI will only make their job easier, so we must redouble our efforts to identify manipulated content and empower the public to identify malicious foreign influence operations.

I look forward to a robust conversation about how the Department of Homeland Security can use AI strategically to carry out its mission more effectively. I look forward to the witnesses' testimony.

Mr. Chairman, I yield back the balance of my time.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MAY 22, 2024

Artificial intelligence is not new. The Department of Homeland Security and its components have a long history of trying to understand how to most appropriately leverage the capacity AI provides.

The release of ChatGPT in November 2022 made clear AI's transformative potential, and it accelerated efforts by the administration and Congress to ensure the United States continues to lead the world on the responsible development and use of AI. As we consider how to deploy AI to better secure the homeland, we must keep 3 critical principles in mind.

First, we must ensure that AI models we use and the data to train them do not reinforce existing biases. That requires that AI used by the Government be developed pursuant to specific policies designed to eliminate bias and is tested and retested to ensure it is not having that effect. Eliminating bias from AI also requires a diverse AI workforce, comprised of people from a variety of backgrounds who can identify potential biases and prevent biases from being encoded into the models.

Second, the Government must rigorously assess appropriate use cases for AI and ensure that the deployment of AI will not jeopardize the civil rights, civil liberties, or privacy of the public. Law enforcement and national security agencies, in particular, must implement an exacting review of potential infringements on these foundational democratic principles.

Moreover, it is essential that the workforce be included in decision-making processes on how AI will be deployed. The workforce is in the best position to understand capability gaps and where AI could add efficiencies. AI is a tool the workforce will use to carry out their jobs more effectively. It is not—and should not ever be—a replacement for people.

Finally, the AI tools we use must be secure. In many respects, existing cybersecurity principles can be adapted to secure AI. I commend the Cybersecurity and Infrastructure Security Agency (CISA) for working with the private sector to ensure the adoption of Secure-by-Design principles in the development of AI. Moving forward, we must determine vulnerabilities unique to AI and work together to address them. I commend President Biden on last year's Executive Order on AI, which put the Federal Government on a path of developing and deploying AI in a manner consistent with these principles.

As DHS continues to assess how it will use AI to carry out its vast mission set—from cybersecurity to disaster response to aviation security—I am confident that it will do so in a manner that incorporates feedback from the workforce and protects civil rights, civil liberties, and privacy. We cannot allow our optimism about the benefits of AI to short-circuit how we evaluate this new technology. At the end of the day, bad technology is bad for security.

As we consider the potential benefits AI presents for DHS's mission, we must also consider the new threats it poses. AI in the hands of our adversaries could jeopardize the security of Federal and critical infrastructure networks as well as the integrity of our elections. We know that China, Russia, and Iran have spent the past 4 years honing their ability to influence our elections, sow discord among the American public, and undermine confidence in our elections results. Advances in AI will only make their job easier, so we must redouble our efforts to identify manipulated content and empower the public to identify malicious foreign influence operations.

I look forward to a robust conversation about how the Department of Homeland Security can use AI strategically to carry out its mission more effectively.

Chairman GREEN. I want to thank the Ranking Member for his comments.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Honorable Jackson Lee follows:]

STATEMENT OF HONORABLE SHEILA JACKSON LEE

MAY 22, 2024

Chairman Green, and Ranking Member Thompson, thank you for holding today's hearing on "Advancing Innovation (AI): Harnessing Artificial Intelligence to Defend and Secure the Homeland."

I look forward to the questions that will follow the testimony of:

- Mr. Troy Demmer, co-founder and chief product officer, Gecko Robotics;

- Mr. Michael Sikorski, CTO and VP of engineering at Palo Alto Networks Unit 42, Palo Alto Networks;
- Mr. Ajay Amlani, president, head of the Americas, iProov; and
- Mr. Jake Laperruque, deputy director, security and surveillance project, Center for Democracy and Technology (CDT) (*Democratic Witness*).

I welcome the witnesses and thank them for their testimony before the House Homeland Security Committee.

The purpose of this hearing is to explore how the responsible use of AI can support the homeland security mission of the Department of Homeland Security (DHS).

Members of the committee will learn about security challenges created by AI, including how adversaries can leverage AI to target the homeland and how the deployment of AI that does not meet safety or security standards can undermine national security.

There are additional areas of concern that the committee should remain focused on ensuring that AI's development and deployment for civilian agency use is safe, secure, and protects civil rights, civil liberties, and privacy.

Members of the committee will hear perspectives on how DHS and CISA can best implement their responsibilities under President Biden's recent AI Executive Order 14110, on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

Executive Order 14110 represents a comprehensive effort by the Biden administration to maintain U.S. dominance in innovation while ensuring artificial intelligence (AI) reflects U.S. values, including prioritization of safety and security and respect for civil rights, civil liberties, and privacy.

AI is generally understood to mean computerized systems that operate in ways commonly thought to require intelligence.

President Biden's recent Executive Order 14110 defined AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments."

Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

The Executive Order outlines that where practicable, AI security policy should be aligned with existing efforts to strengthen the security of technology, such as secure-by-design.

Given the momentum associated with AI policy, such alignment could help to further accelerate the implementation of such security principles to broader sets of technology while streamlining DHS/CISA guidance.

AI THREATS AND OPPORTUNITIES

Generative AI is being used to generate increasingly realistic photo, audio, and video forgeries, or "deep fakes," that adversaries could deploy as part of an information operation.

Past deep fakes have been detectable by experts; however, the sophistication of the technology is progressing to the point that it may soon be capable of fooling forensic analysis tools.

Additionally, as deep fakes become more realistic they risk undermining public confidence in legitimate video or audio.

Generative AI can also facilitate cyber crimes by helping produce more convincing phishing emails.

According to one report, in the last year, there has been a 1,265 percent increase in malicious phishing emails, suggesting generative AI may be contributing to this significant rise in phishing attacks.

Further, artificial intelligence can be used to create full "digital patterns-of-life," matching digital footprints with purchase histories, credit reports, resumes, and other information to create comprehensive behavioral profiles of Government officials or private citizens.

These digital profiles can unmask people who work in Sensitive to highly-Classified areas of Government and anticipate their movements.

This application of AI can also target elected officials, law enforcement officers, and essential workers in critical infrastructure.

President Biden has taken important actions to support research and development in AI and to ensure that AI development is secure, safe, and respects civil rights and privacy concerns.

In October 2022, the White House Office of Science and Technology Policy released the Blueprint for an AI Bill of Rights, a non-binding document designed to lay out key principles and policies to ensure AI development protects civil rights and promotes democratic values.

On October 30, 2023, President Biden issued an Executive Order on “Safe, Secure, and Trustworthy Artificial Intelligence”, and during the first few months of 2024, the Biden administration secured voluntary commitments from 15 leading AI companies to follow certain policies designed to manage risks posed by AI.

AI’s goal is to replace many tasks performed by humans with machines, but the consequences for human error and computing error are not the same.

Human errors are costly and borne by the person or the company they represent, while a computer error is borne by the purchaser not the manufacturer.

This situation in an AI world would create incentives to replace people with machines that are not held to the same standards of care as people.

While precise definitions vary, President Biden’s recent Executive Order 14110 defined AI as “a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.”

The EO also issues several mandates for DHS.

It directs DHS to establish an AI Safety and Security Board consisting of private- and public-sector experts to issue recommendations and best practices to ensure AI deployments are secure and resilient.

It also directs CISA to partner with sector risk management agencies to conduct AI risk assessments for each critical infrastructure sector.

Additionally, DHS will update existing security guidance to incorporate NIST’s AI Risk Management Framework and will conduct a pilot on utilizing AI to discover and remediate vulnerabilities on Federal agency networks.

CISA will also support the Office of Management and Budget’s effort to issue guidance to agencies on red-teaming generative AI systems.

Outside of AI security, DHS also has key tasks related to facilitating immigration pathways for AI experts and leading efforts to combat AI intellectual property theft.

DHS/CISA ACTIONS ON AI

Shortly after President Biden signed the EO, CISA released its 2023–2024 Roadmap for Artificial Intelligence, which describes the 5 lines of effort the agency will undertake to action its obligations under the Executive Order:

- Responsibly Use AI to Support [CISA’s] Mission;
- Assure AI Systems;
- Protect Critical Infrastructure from Malicious Use of AI;
- Collaborate with and Communicate on Key AI Efforts with the Interagency, International Partners, and the Public; and
- Expand AI Expertise in our Workforce.

CISA’s Roadmap wisely leverages existing programs and policies to address AI security issues where possible while developing new policies and work streams where gaps in policies exist.

Some of the more specific objectives CISA seeks to implement under its Roadmap include developing a strategy to adopt the next generation of AI-enabled technologies; generating best practices on the development and use of secure AI systems; engaging with international partners on global AI security; and recruiting staff with AI expertise.

In line with CISA’s commitment to international cooperation on AI policy and its goal of providing guidance on best practices for the private sector, last month, CISA and the United Kingdom’s National Cyber Security Centre jointly released Guidelines for Secure AI System Development in collaboration with agencies from 16 other countries.

The guidelines focused on securing all aspects of the AI development life cycle, including secure design, secure development, secure deployment, and secure operation and maintenance.

The publication aligns with CISA’s broader focus on encouraging software developers to follow secure-by-design principles that ensure security is built into the technology product development process.

As DHS increases its use of AI across its components and missions, in April of this year, Secretary Mayorkas established the DHS AI Task Force, which seeks to drive the use of AI across DHS while protecting civil rights, civil liberties, and privacy.

The task force is chaired by the Department’s chief AI officer and the under secretary for science and technology, with the officer for civil rights and civil liberties serving as vice chair.

Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

This assumes that AI's human-based inputs function as intended free from errors or omissions.

Contracting and service agreements on the adoption and use of AI should consider important lessons learned from the *healthcare.gov* experience—tens of millions were lost due to poor contract management.

For this reason, the management of AI development for civilian agencies or critical infrastructure use is as important as the applications that being developed.

AI OPPORTUNITIES

AI offers a wide range of potential applications across different sectors.

In cybersecurity, AI has largely worked to the advantage of network defenders.

For example, conventional cybersecurity tools defend against known matches to malicious code, so hackers must modify small portions of that code to circumvent the defense.

AI-enabled tools, on the other hand, can be trained to detect anomalies in network activity, thus presenting a more comprehensive and dynamic barrier to attack.

In the aftermath of the 2020 Solar Winds cyber campaign, Federal agencies and the private sector have expedited implementation of Endpoint Detection and Response systems that utilize AI to detect anomalous network activity.

However, AI has and will continue to be used in myriad ways that undermine national security, individual privacy, or introduce new and novel attack vectors.

Rapid advances in generative AI, as highlighted by the release of ChatGPT in November 2022, have increased concerns about how more advanced versions of AI may increase security risks.

Generative AI means the class of AI models that emulate the structure and characteristics of input data in order to generate derived synthetic content.

This can include images, videos, audio, text, and other digital content.

There will be no one definition of AI or one method that defines what it is or what it will mean.

The efforts behind AI are focused on may not be able to plan for all possible outcomes, but one that may make this conversation much more challenging is the creation of machines that can write their own computing code or algorithms without human intervention will quickly lead to code that is only understood by AI.

The Biden administration's efforts, including EO 14110, reflect major advances in Federal AI policy and full implementation of those policies, in consultation with private-sector experts and stakeholders, offer the potential to strengthen national security while mitigating the novel risks posed by AI.

AI can be made to accomplish a great deal if we are not complacent in the effort to build better AI for civilian agencies and critical infrastructure use.

AI can be trained.

AI can be tested.

We must leverage these 2 facts to ensure that tax dollars on AI systems and applications are not wasted or lost to fraud and abuse.

I plan to introduce legislation specifically addressing civilian agency use and critical infrastructure to focus efforts on building a sound model for AI adoption.

Thank you.

Chairman GREEN. I am pleased to have a distinguished panel of witnesses before us today, and I ask that our witnesses please stand and raise your right hand.

[Witnesses sworn.]

Chairman GREEN. Let the record reflect that the witnesses have answered in the affirmative. Thank you. Please be seated.

I would now like to formally introduce our witnesses. Mr. Troy Demmer is the co-founder and chief product officer at Gecko Robotics, a company combining advanced robotics and AI-powered software to help ensure the availability, reliability, and sustainability of critical infrastructure.

Today Gecko's innovative climbing robots capture data from the real world that was never before accessible. From pipelines, ship hulls, missile silos, and other critical asset types. Gecko's AI-driven software platform then enables human experts to contextualize that data and translate it into operational improvements.

Mr. Michael Sikorski is Palo Alto Networks' Unit 42's chief technology officer and vice president of engineering. He has over 20 years of experience working on high-profile incidents and leading research and development teams, including at Mandiant and National Security Agency. Mr. Sikorski is also an adjunct assistant professor for computer science at Columbia University.

Mr. Ajay Almanai—how do you pronounce your name, sir?

Mr. AMLANI. Ajay Amlani.

Chairman GREEN. Ajay Amlani. Got it, thank you. He currently serves as the president and head of the Americas for iProov, a global provider of biometric authentication products used for on-line enrollment and verification. In addition, he is a well-recognized identity technology expert serving as a strategic advisor for industry leaders working in artificial intelligence, identity technology, and ecommerce.

Mr. Jake Laperruque is the deputy director of the Center for Democracy and Technology, Security and Surveillance Project. Prior to joining CDT, Jake worked as senior counsel at the Constitution Project at the Project on Government Oversight. He also previously served as a program fellow at the Open Technology Institute and law clerk of the Senate Subcommittee on Privacy, Technology, and the Law.

Again, I thank our witnesses for being here, and I now recognize Mr. Demmer for 5 minutes to summarize his opening statement.

STATEMENT OF TROY DEMMER, CO-FOUNDER AND CHIEF PRODUCT OFFICER, GECKO ROBOTICS

Mr. DEMMER. Good morning, Chairman Green, Ranking Member Thompson, and Members of the committee. Thank you for the opportunity to join you today. My name is Troy Demmer, and I am the co-founder of Gecko Robotics, a Pittsburgh-based technology company that uses robots, software, and AI to change how we understand the health and integrity of physical infrastructure.

Back in 2013, Gecko started with a problem. A power plant near where my cofounder and I went to college had to keep shutting down due to critical assets failing. The problem was obvious from the first meeting with the plant manager: They had almost no data.

The data that had been collected was collected very manually with a gauge reader at a single point and sensor measurement. Furthermore, that data was often collected by workers working off of ropes at elevated heights or in confined spaces resulting in few measurement readings. That meant the power plant had to make reactive decisions rather than being proactive.

That was the genesis of the idea behind Gecko, using rapid technological advances in robots, software, and AI to get better data and generate better outcomes. We do this by building wall-climbing robots armed with various sensor payloads that can gather 1,000 times more data at 10 times the speed compared to traditional methods.

We also have a software platform that takes that data and combines it with other data sets to build a first order understanding of the health of critical infrastructure. Where are the vulnerabilities? What do we need to do to be proactive before fixing it before a problem occurs? How do we prevent catastrophic disasters?

Those are the problems Gecko is solving today for some of the most critical infrastructure that protects the American way of life. We're helping the Navy reduce their maintenance backlog and build the next generation of military equipment smarter.

We're helping the U.S. Air Force create the digital baseline for the largest infrastructure program since the Eisenhower interstate highway project. We're working with various other critical public and commercial infrastructure projects across the country. In every one of these cases the missing link is the data, and that brings us to the conversation we're having in today's hearing.

AI models are only as good as the inputs they are trained on. Trustworthy AI requires trustworthy data inputs, data inputs that are auditable, interrogatable. Data inputs that provide the complete and undiluted answer to questions we are asking. When it comes to our critical infrastructure, infrastructure that powers the American way of life and protects our homeland, those data inputs for the most part do not exist.

Without better data even the most sophisticated AI models will be at best ineffective and at worst harmful.

Yet the way America collects data on infrastructure today hasn't fundamentally changed in 50 years. Today, despite advances in data collection technologies like robots, drones, fixed sensors, and smart probes that can detect corrosion through layers of concrete, we are still largely gathering data manually even on our most critical infrastructure like dams, pipelines, bridges, power plants, railroads, and even military assets.

To give you one example from our work, we have one major national security partner who collects data on critical assets both manually and with our robots. Their manual process collected by handheld sensors and skateboards creates 3,000 individual data points. Our robots on that same asset collect more than 8 million.

That is more than 2,600 times the data, data that multiplies the power of AI models and their predictive value. That's the scale and of the difference between new technology-driven processes and manual processes that we still largely rely on to secure our critical infrastructure.

Without better data collection AI will never meet its potential to secure the critical infrastructure that protects our homeland and the American way of life.

As I conclude, I want to touch briefly on how we think about robotics and AI in the work force construct. At Gecko we talk a lot about upskilling the work force. That's a big priority for many of our partners.

We've responded by hiring a significant number of former manual inspector workers and then training them to operate our robots. More than 20 percent of our employees don't have 4-year degrees. Workers who once hung from ropes at dangerous heights are now operating robots. Workers who built their careers inspecting assets are now helping our software developers build the tools to make that work better.

Thank you again for the opportunity to join you today, and I look forward to your questions.

[The prepared statement of Mr. Demmer follows:]

PREPARED STATEMENT OF TROY DEMMER

MAY 22, 2024

Good morning, Chairman Green, Ranking Member Thompson, and Members of the House Committee on Homeland Security. On behalf of Gecko Robotics and our 250+ employees in Pennsylvania, Massachusetts, Texas, New York, North Carolina, South Carolina, and around the world, I would like to thank you for inviting me to testify before you today.

My name is Troy Demmer, and I am the co-founder of Gecko Robotics, a Pittsburgh-based technology company that uses robotics, software, and AI to change how we understand the health and integrity of physical infrastructure.

My testimony today will focus on the missing ingredient preventing AI from being an effective tool for securing the physical infrastructure that powers the American way of life and protects our Nation—the data.

Fifty years ago, we assessed the health of physical infrastructure by taking manual data readings. Today, despite advances in data collection technologies (robots that can climb, fly, and swim; probes that can detect steel corrosion through layers of concrete), we are still largely gathering data manually—even on our most critical infrastructure like dams, bridges, power plants, railroads, and even military assets. This manually-collected data is low quality and low quantity, giving us little insight into the health of our infrastructure.

Back in 2013, we started Gecko Robotics to solve this exact problem. A power plant near where my co-founder and I went to college kept shutting down due to critical failures. Unscheduled plant shutdowns have a cascading effect on the local power grid and surrounding communities. Utilities have to find power elsewhere and buy it at higher rates—and those costs are passed on to consumers. As was the industry standard at the time, the plant was regularly collecting data manually. This low-quality, low-quantity data was not only ineffective at helping them prevent shutdowns; collecting it often required workers to hang from ropes at dangerous heights. Without high-quality, high-quantity data on their critical infrastructure, the power plant could not avoid failures. They were forced to react to problems rather than prevent them.

Why does this matter in a hearing on “Harnessing Artificial Intelligence to Defend and Secure the Homeland”? Because AI models that apply to physical infrastructure are designed to do just that—to prevent problems before they happen. The right application of AI should be able to tell you exactly how to operate a power grid or the vulnerabilities of a dam or bridge. But even the best AI applications are only as good as the data they are trained on. Trustworthy AI requires trustworthy data inputs—data inputs that are auditable and interrogatable. As much as data is important to cybersecurity and our Nation’s virtual infrastructure, it’s also important to our physical infrastructure. Without the data, no amount of AI can help us secure and defend this infrastructure against vulnerabilities that threaten our way of life.

Those of us working on this problem understand its importance and are investing in building technologies that will solve it. Most people are focused on building solutions that are realistically 10 years away from mission readiness. But our critical infrastructure is failing today. Bridges are collapsing. Power plants are failing. Ships are corroding. AI can help, but only if it has the right data. We need a solution not only for the future, but also for today.

When it comes to harnessing AI to secure and defend our critical infrastructure, we face two issues: First, most AI efforts are not focused on gathering data and building AI for the built world—and they are building for tomorrow, not today. And second, most AI development efforts are focused on software even though hardware is just as important to supporting AI.

As the committee decides how best to harness AI, I encourage you all to consider two key points:

(1) AI efforts must focus on gathering high-fidelity data not only to support cybersecurity but to support infrastructure security, as well

(2) Developing cutting-edge data acquisition hardware is critical to creating AI technology that secures and protects our infrastructure.

INVEST IN DATA FOR AI PROGRAMS DESIGNED FOR THE BUILT WORLD

When we think of defending the homeland via AI, we typically focus on cyber threats and digital infrastructure. However, physical infrastructure—bridges, tunnels, railways, power plants, pipelines, shipping vessels, and more—forms the backbone of our Nation's security. Like cyber infrastructure, these assets are susceptible to threats and degradation over time. Advanced AI systems can analyze data collected from sensors and robotic systems to secure our critical infrastructure—but only if we have the data.

The American Society of Civil Engineers' most recent Report Card gave American infrastructure a bleak C− rating.[1] Digging into the scores presents an even bleaker picture. American transit earned a D−. American dams, levees, roads, and stormwater systems all received Ds. These poor grades not only reflect the quality of our infrastructure today. They also reflect the quality of the data we have about that infrastructure.

This lack of data is alarming, because the less data we have, the less insight we have and the more vulnerable we are when there's a threat. If a cyber attack took down a major power plant, how hard can we run all of our back-up generators and other electrical assets without causing a major blackout? Today, we don't know.

And cyber attack isn't the only threat our infrastructure faces. Natural degradation of this infrastructure also threatens our national security. The Federal Emergency Management Agency (FEMA) estimates there are approximately 15,600 dams in the United States with a high hazard potential, meaning their failure could result in loss of life.[2] Across the country, there are 167 million daily crossings on bridges rated to be in "poor" condition.[3] In fact, Gecko Robotics' headquarters was just miles away from where the Fern Hollow Bridge collapsed in 2023, injuring 10 and requiring $25.3 million to rebuild.[4] Recent climate studies estimate that a mass electrical blackout that coincides with a brutal summer heatwave could more than double heat-related deaths in major U.S. cities.[5]

Failure of these assets would be catastrophic, but we lack data on how best to maintain them or respond during times of crisis. That's because today, data is still collected by hand with scaffolding and solitary sensors. Today, railroad companies use wax sticks to judge if train tracks are too hot for operation. The result? We can't make confident maintenance or crisis-time decisions.

Modern tools are so easy to use that any high school kid can build an AI model with a few lines of code. But inputs matter. Because of this, the very first question that you should ask as agencies implement AI is, "How was this data collected, and can I trust it?"

I urge this committee to prioritize identifying and collecting the right data and pursuing AI programs that stress the importance of data. The more accurate and relevant the data, the more effective our AI solutions will be at enhancing infrastructure security.

UPDATE FUNDING PROGRAMS TO ACCOUNT FOR HARDWARE DEVELOPMENT

To collect AI-quality data about our physical infrastructure, we need to invest in data acquisition systems like sensors and robots; however, companies like Gecko face three key obstacles to developing these kinds of systems because of the way current Government funding programs are designed.

(1) The first obstacle is that most funding programs do not account for the upfront investment required to develop these systems. To develop and test our robots, Gecko Robotics has built an industrial testing environment complete with sample boiler tubes, tank shells, and concrete missile silos. Our internal development of testing environments has been key to our ability to rapidly test and prototype our technology. Under Executive Order 14110, DHS is an important partner in "developing and helping to ensure the availability of testing environments, such as test beds, to support the development of safe, secure, and trust-

[1] Report Card for America's Infrastructure (2021). American Society of Civil Engineers (ASCE). *https://infrastructurereportcard.org/*.

[2] FEMA National Dam Safety Program Overview (2021). Federal Emergency Management Agency. *https://www.fema.gov/sites/default/files/documents/fema_nsdp-overview-fact-sheet.pdf*.

[3] Bridge Report (2024). American Road & Transportation Builders Association. *https://artbabridgereport.org/state/map*.

[4] $25.3M in Federal funding set aside to replace Pittsburgh's collapsed Fern Hollow Bridge (2022). Trib Total Media. *https://triblive.com/local/25-3m-in-Federal-funding-set-aside-to-replace-pittsburghs-collapsed-fern-hollow-bridge/*.

[5] How Blackouts during Heat Waves Amplify Mortality and Morbidity Risk (2023). Stone et. al. Journal of Environmental Science and Technology. *https://doi.org/10.1021/acs.est.2c09588*.

worthy AI technologies . . . ".[6] I urge DHS to provide access to adequate testing environments for qualified companies—a critical step in developing AI for physical infrastructure.

(2) The second obstacle is that some funding programs don't account for the ways hardware is developed. Unlike software, which can be rapidly prototyped and scaled, hardware development often demands more engineering staff and longer testing periods. We need programs that recognize and account for the unique requirements of hardware development. For example, programs like DHS's Silicon Valley Innovation Program (SVIP) provide huge opportunities to develop hardware systems that can drive the development of safe and reliable AI for national security. However, the current headcount (<200 FTE) and funding (<$1 million in Federal contracts) requirements limit the ability of hardware-focused start-ups to participate.

(3) The third obstacle is that many hardware—and software—start-ups are backed by venture capitalists (VCs), including almost all start-ups that develop and deploy AI. However, DHS's Small Business Innovation Research (SBIR) program has, to date, not opted into the "Majority VC ownership" authority (as specified in 15 U.S.C 638(dd)).[7] This means that many VC-backed companies developing AI or AI-enablement technologies are ineligible to apply to this competitive program. As a recipient of SBIR awards from the Department of Defense—which has opted into majority VC ownership authority—Gecko has seen first-hand how non-dilutive, early stage funding to VC-backed start-ups advances the priorities of both the U.S. Government and small businesses. I encourage DHS to opt into this authority.

Hardware innovation is foundational to gathering the high-fidelity data needed to build safe and reliable AI—especially AI capable of maintaining our aging infrastructure. By integrating hardware research and development (R&D) into funding programs for AI development, we can foster the data acquisition ecosystems that support effective AI for our physical infrastructure.

CONCLUSION

AI holds tremendous potential to change how we understand, optimize, and defend the most critical physical infrastructure our Nation relies on. But without an emphasis on collecting the right quality and quantity of data, most of that potential will likely never materialize. By fostering data-focused policies, programs, and partnerships for industry, the Government can promote the responsible collection of data to power reliable AI models. Further, by centering AI programs around the built world and providing the necessary resources for cutting-edge hardware development, we can significantly enhance our Nation's security posture.

Thank you for your time and consideration.

Chairman GREEN. Thank you, Mr. Demmer.

I now recognize Mr. Sikorski for 5 minutes to summarize his opening statement.

STATEMENT OF MICHAEL SIKORSKI, CHIEF TECHNOLOGY OFFICER AND VICE PRESIDENT OF ENGINEERING, UNIT 42, PALO ALTO NETWORKS

Mr. SIKORSKI. Chairman Green, Ranking Member Thompson, and distinguished Members of the committee, thank you for the opportunity to testify in the critical role that artificial intelligence plays in enhancing cybersecurity defenses and securing the homeland.

My name is Michael Sikorski and I am the chief technology officer and vice president of engineering for Unit 42, which is the threat intelligence and incident response division of Palo Alto Networks. For those not familiar with Palo Alto Networks, we are an

[6] Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023). Executive Office of the President. *https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.*

[7] VC Ownership Authority (Accessed May 17, 2024). Small Business Innovation Research. *https://www.sbir.gov/vc-ownership-authority.*

American-headquartered company founded in 2005 that has since become the global cybersecurity leader.

We support 95 of the Fortune 100, the U.S. Federal Government, critical infrastructure operators, and a wide range of State and local partners. This means that we have deep and broad visibility into the cyber threat landscape. We are committed to being trusted national security partners with the Federal Government.

As my written testimony outlines, AI is central to realizing this commitment. We encourage everyone to embrace AI's transformative impact for cyber defense. A reality of today's threat landscape is that adversaries are growing increasingly sophisticated, and AI will further amplify the scale and speed of their attacks.

However, this fact only heightens the importance of maximizing the substantial benefits that AI offers for cyber defense. The AI impact for cyber defense is already very significant.

By leveraging precision AI, each day Palo Alto Networks detects 2.3 million unique attacks that were not present the day before. This process of continuous discovery and analysis allows threat detection to stay ahead of the adversary, blocking 11.3 billion total attacks each day and remediating cloud threats 20 times faster.

The bottom line is that AI makes security data actionable for cyber defenders, giving them real-time visibility across their digital enterprises, and the ability to prevent, detect, and respond to cyber attacks quickly.

Accordingly, Palo Alto Networks firmly believes that to stop the bad guys from winning we must aggressively leverage AI for cyber defense. My written testimony highlights a compelling-use case of AI-powered cybersecurity that is showing notable results up-leveling and modernizing the Security Operation Center, also known as the SOC.

For too long, the cybersecurity community's most precious resources, our people have been inundated with alerts to triage manually. This creates an inefficient game of Whac-A-Mole while critical alerts are missed and vulnerabilities remain exposed.

We have seen transformative results from customer use of AI-powered SOCs. This includes the following: a reduction of mean time to respond from 2 to 3 days down to under 2 hours; a 5 times increase in incident closeout rates; and a 4 times increase in the amount of security data ingested and analyzed each day.

Outcomes like these are necessary to stop threat actors before they can encrypt systems or steal sensitive information, and none of this would be possible without AI. This new AI-infused world we live in also necessitates what we like to call secure-AI-by-design.

Organizations will need to, No. 1, secure every step of the AI application development life cycle and supply chain; No. 2, protect AI data from unauthorized access and leakage at all times; and No. 3, oversee employee AI usage to ensure compliance with internal policies.

These principles are aligned with and based on the security concepts already included in the NIST AI risk management framework and should be promoted for ecosystem-wide benefit.

Now, the issues we're discussing today are important to me also on a personal level. I'm honored to have spent decades both as a cybersecurity practitioner partnering with governments to stop threats and as an educator training the cyber work force of tomorrow.

It's with that background that I can say confidently that homeland security, national security, and critical infrastructure resilience are being enhanced by AI-powered cyber defense as we speak, and we must keep the pedal to the metal because our adversaries are not, certainly not, sitting on their hands.

Thank you again for the opportunity to testify, and I look forward to your questions and continuing this important conversation.

[The prepared statement of Mr. Sikorski follows:]

PREPARED STATEMENT OF MICHAEL SIKORSKI

MAY 22, 2024

Chairman Green, Ranking Member Thompson, and distinguished Members of the committee:

Thank you for the opportunity to testify on the critical role that artificial intelligence (AI) plays in enhancing cybersecurity defenses. Your commitment to exploring the homeland security benefits of AI-powered cyber defense is commendable. My name is Michael Sikorski, and I am the chief technology officer and vice president of engineering at Unit 42, the threat intelligence and incident response division at Palo Alto Networks.

For those not familiar with Palo Alto Networks, we were founded in 2005 and have since become the global cybersecurity leader—protecting over 65,000 enterprises across more than 150 countries. We support 95 of the Fortune 100, critical infrastructure operators of all shapes and sizes, the U.S. Federal Government, universities and other educational institutions, and a wide range of State and local partners.

At Palo Alto Networks, we have a unique vantage point into the cyber threat landscape. What we see on a daily basis is concerning. Adversaries are growing increasingly sophisticated, and AI is amplifying the scale and speed of their attacks.

This backdrop only heightens the importance of fully harnessing the substantial benefits AI offers for cyber defense. Indeed, the demonstrated impact of AI-powered cyber defense is already significant. By leveraging AI, each day Palo Alto Networks detects 2.3 million unique attacks that were not present the day before. This process of continuous discovery and analysis allows threat detection to stay ahead of the adversary, blocking 11.3 billion total attacks every day with 20 times faster triage and remediation speeds in the cloud.

Results like these underscore why Palo Alto Networks firmly believes the risky outcome for society would be not aggressively leveraging AI for cyber defense purposes. AI makes security data actionable for network defenders, giving them real-time visibility across their digital enterprises and the ability to prevent, detect, and respond to cyber attacks quickly. We look forward to working with policy makers to further promote the adoption of AI for this important use case.

STAYING VIGILANT AGAINST THE EVOLVING THREAT LANDSCAPE

Cyber adversaries are already leveraging AI to advance their tradecraft and will continue to do so going forward. For example, we see evidence that adversaries are using AI to enhance what we call social engineering attacks—phishing emails designed to lure users to "click the link." Historically, these messages have been littered with poor grammar and typos, making their fraudulent nature relatively easy to detect, but they are becoming more accurate and therefore more believable. Adversaries are now able to generate flawless, mistake-free text, enabling click-through rates to skyrocket.

Additionally, bad actors are innovating with AI to accelerate and scale attacks and find new attack vectors. They can now execute numerous simultaneous attacks on one company across multiple vulnerabilities. Adversarial use of AI allows faster lateral movement within networks and more rapid weaponization of reconnaissance data. Going forward, there is the potential for a significant surge in malware variants as the cost of creating customized malware drops substantially.

None of this should be a surprise. Adversaries are always evolving, with or without AI, and we can never be complacent. As cyber defenders, our mission is to understand and track adversarial capability while relentlessly innovating and deploying best-in-class security tools to stay ahead.

LEVERAGING AI FOR CYBER DEFENSE

Despite the evolving threat landscape, we remain confident that we are well-equipped to combat the cyber incursions of today and tomorrow. AI is, and will continue to be, a game-changer to help cyber defenders ward off the crooks, criminals, and nation-states that threaten our digital way of life. AI supercharges cyber defenses and helps anticipate, track, and thwart cyber attacks to a degree never seen before.

Our product suite, which spans network security, cloud security, endpoint security, and Security Operations Center (SOC) automation, leverages AI to stay a step ahead of attackers.

We first introduced machine learning (ML) capabilities as part of our malware protection offering 10 years ago and have continued to augment our capabilities with AI tools. We now deploy over 30 products that leverage AI, with many more in development. Just this month, we introduced Precision AI™, combining the best of ML, deep learning, and generative AI to achieve real-time and automated security.

The continued investment in and integration of AI into cyber defense capabilities is important because it provides defenders a more capable and nimble tool kit to analyze security data—yielding powerful insights that guide deployment of protective measures.

AI-POWERED CYBER DEFENSE IN ACTION—SIGNIFICANT BENEFITS FOR DEFENDERS

For too long, our community's most precious cyber resources—people—have been inundated with security alerts that require manual triage, forcing them to play an inefficient game of "whack-a-mole," while vulnerabilities remain exposed and critical alerts are missed. Making matters more difficult, this legacy approach often requires defenders to stitch together security data from across dozens of disparate cybersecurity products at the same time, a difficult task often counterproductive to achieving desired cybersecurity outcomes. Organizations find themselves drowning in their own data, struggling to operationalize it. Industry research shows that over 90 percent of SOCs are still dependent on manual processes, a sure-fire way to give adversaries the upper hand.

This inefficient, manual posture results in suboptimal Mean Time to Detect and Mean Time to Respond times for security operations teams. As the terms suggest, these metrics provide quantifiable data points for network defenders about how quickly they discover potential security incidents and then how quickly they can contain them. Historically, organizations have struggled to execute against these metrics. In fact, a recent report by Unit 42 found that security teams average nearly 6 days to resolve an alert in cloud breach incident response cases. However, we are now seeing attackers exfiltrate data in under a day in almost 50 percent of all incident response cases. As recently as just a few years ago, attackers were taking over a week to exfiltrate data after compromise.

AI-Driven Security Operations Centers

AI-driven SOCs can flip this paradigm and give defenders the upper hand. This technology acts as a force multiplier for cybersecurity professionals to substantially reduce detection and response times.

The results from deploying this technology on our own company networks are significant:

- On average, we ingest 59 billion events daily.
- Using AI-driven data analysis, this is distilled down to 26 thousand raw alerts.
- This is further triaged to just 75 that require further analysis.

We then deployed this AI-powered SOC to our customers where we are seeing similarly transformative outcomes:

- Reduction of Mean Time to Respond from 2–3 days to under 2 hours.
- Five-fold increase in incident close out rate.
- Four-fold increase in the amount of security data ingested and analyzed each day.

These dramatic improvements are critical to stopping threat actors before they can encrypt systems or steal sensitive information. None of this would be possible without the power of AI.

AI-Powered Copilots to Optimize Security Outcomes

Finding ways to radically simplify cybersecurity puts network defenders in a position to succeed. AI-powered copilots introduce the ability for practitioners to more seamlessly interact with their security tools—asking questions in natural language and yielding many operational advantages. Specifically, copilots can answer "how to" questions, provide easy explanations to complex security challenges, provide step-by-step guidance, generate precise product queries, and create visual responses.

From the copilots we have already deployed, it is clear that they are a force multiplier for defenders—surfacing the most important security tasks, explaining why they are critical, and more importantly, expediting remediation.

SECURING AI BY DESIGN

AI is here to stay. In fact, 42 percent of enterprises are already leveraging AI tools, and this is expected to grow to 96 percent within the next 12 months.

The typical large enterprise will use hundreds of AI apps internally, leverage thousands of AI models, and produce many petabytes of training and vector embedding data annually.

However, this expanded AI attack surface does not come without data security and network security challenges. Research indicates that 50 percent of employees currently use AI apps without permission in their enterprise, 80 percent of public models can be "jailbroken" (bypassing restrictions installed by model creators), and there are already hundreds of malicious models available in the wild.

In sum, AI app proliferation is changing how enterprises operate and necessitates an evolved security approach. We like to think of this approach as Securing AI By Design. This approach requires the ability to:

(1) Secure every step of the AI app development life cycle and supply chain.

(2) Protect AI applications, models, and data from threats in run time.

(3) Oversee employee AI usage to ensure compliance with internal policies.

These principles are aligned with—and based on—the security concepts already included in the NIST AI Risk Management Framework (RMF). Palo Alto Networks would welcome the opportunity to continue engaging with Members of the committee and staff about how we can promote these principles for ecosystem-wide benefit.

MAXIMIZING AI'S POTENTIAL FOR CYBER DEFENSE

We offer the following considerations for policy makers as we look to further encourage the deployment of AI-powered solutions for cyber defense:

(1) *Promote Federal Government Leadership*.—The power of Federal procurement can drive behavior across a wide range of cybersecurity stakeholders. Accordingly, we encourage the Federal Government to continue to lean into the promotion of AI-enabled cyber defense. To that end, Palo Alto Networks is encouraged to see a dedicated section in the most recent version of bipartisan FISMA reform legislation that specifically calls on OMB to produce guidance promoting AI's use "wherever automation is used in furtherance of the cybersecurity of information systems." This is an important provision that we enthusiastically support.

(2) *Build Upon Flexible Frameworks*.—The NIST AI RMF serves as a thoughtfully-crafted baseline for understanding AI risk that can act as the cornerstone for any organization. The RMF allows organizations to assess their needs and capabilities against the varied circumstances in which they use, develop, or deploy AI systems—evaluating both the risks and benefits of those systems.

(3) *Embrace Secure AI By Design*.—As outlined in greater detail above, enterprises will benefit from capabilities that assist in inventorying AI usage, applying policy controls, and securing apps built with AI.

(4) *Differentiate Between Use Cases, Impacts, and Data Types*.—We believe policy makers should employ a risk-based approach when considering AI guardrails that takes into account differences in the use cases, the data processed in those use cases, and the potential resulting impacts on individuals. There are fundamental differences in risk between AI systems that leverage consumer data to make or facilitate consequential decisions with human impact—such as college admissions or loan approvals—and those systems that leverage security data to ensure the robustness and resilience of networks.

(5) *Ensure Disclosure Requirements Do Not Have Unintended Consequences*.—Palo Alto Networks recognizes that impact assessments and risk management disclosures for AI models are increasingly being proposed to improve AI transparency. We urge policy makers to take into account the potential national security impact when formulating the details of disclosure requirements. For example, public disclosures that require information detailing how network defenders use and train AI systems to secure networks could unintentionally create a road map for cyber adversaries to break through those defenses, in turn jeopardizing the underlying security of network and information systems.

PEOPLE AND PARTNERSHIPS

With AI and automation central to modern cyber defenses, we must educate and train the cyber workforce with the advanced skills required for meaningful jobs that complement technological innovation. This is essential to staying ahead of all cyber threats.

As an educator myself, I am personally passionate about expanding access to cyber education at young ages and finding innovative ways for Government and industry to work together to prepare future generations.

To that end, our company is encouraged to see the impact of several initiatives aimed at broadening access to cybersecurity education, including the Palo Alto Networks Cybersecurity Academy, which offers free and accessible curricula aligned to the NIST National Initiative for Cybersecurity Education (NICE) Framework, to academic institutions from middle school through college. Hands-on experiences with cyber and AI benefit the entire ecosystem as they help to upskill our own workforce as well as that of our customers.

Palo Alto Networks also offers several accelerated on-boarding programs to help diversify our workforce, including the Unit 42 Academy. As full-time members of our incident response and cyber risk management teams, early career professionals with both university and military backgrounds spend 15 months developing skills through specialized, instructor-led courses, on-the-job training, and mentorship. We are proud to report that our 2023–2024 class is 80 percent female.

Partnership is in our DNA at Palo Alto Networks and our collective defense depends upon deepening collaboration between industry and Government. We continue to see productive collaboration take place across a range of cybersecurity-focused convening bodies, including CISA's Joint Cyber Defense Collaborative (JCDC), the National Security Telecommunications Advisory Committee (NSTAC), and the Information Technology Sector Coordinating Council (IT–SCC), where we serve as members. We are also an active participant in the DHS ICT Supply Chain Risk Management Task Force. We maintain robust threat intelligence sharing partnerships with DHS, the NSA Cyber Collaboration Center, the Cyber Threat Alliance (whose board I serve on), and other entities to share technical threat data and collaborate to support Government and industry response to significant cyber incidents.

We take our partnership with law makers—and this committee—seriously. Please consider Palo Alto Networks a standing resource as you continue to consider cybersecurity and AI policy issues.

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

Chairman GREEN. Thank you, Mr. Sikorski.

I now recognize Mr. Amlani for his 5 minutes of opening statement.

STATEMENT OF AJAY AMLANI, PRESIDENT, HEAD OF AMERICAS, iPROOV

Mr. AMLANI. Good morning, Chairman Green, Ranking Member Thompson, and Members of the committee. My name is Ajay Amlani and I've been building innovative solutions to help organizations assure people's identities for the last 20 years. I serve as president and head of Americas at iProov.

I started my Federal service as a White House fellow and senior policy adviser to Secretary Tom Ridge, the first Secretary of Homeland Security in the aftermath of the 9/11 attacks at a time in which the Federal Government was rethinking how to manage its national security missions. A large part of that included finding new ways to benefit from the innovation happening in the private sector.

For the past 20 years I have forged partnerships with the Federal Government and the commercial sector that facilitate the utilization of commercial technology to augment national security initiatives.

Today, this committee is considering how to harness the power of AI as part of a multilayered defense against our adversaries. To best answer this question we need to start with understanding how AI enables threat actors. What capabilities can DHS and its component agencies develop to combat these threats? What actions can the Department take to better work with industry as it promotes standards for AI adoption?

AI exponentially increases the capabilities and the speed to deploy new fraud and cyber attacks on the homeland. They enable new threat technology developers to dramatically shorten their innovation cycles.

Ultimately, AI technologies are unique in the way that they upskill threat actors. The actors themselves no longer have to be sophisticated. AI is democratizing the threat landscape by providing any aspiring cyber criminal easy-to-use advanced tools capable of achieving sophisticated outcomes.

The crime-as-a-service dark web is very affordable. The only way to combat AI-based attacks is to harness the power of AI in our cybersecurity strategies. At iProov we developed AI-powered biometric solutions to answer a fundamental question. How can we be sure of someone's identity? iProov is trusted by governments and financial institutions globally to combat cyber crime by verifying that an individual is not only the right person but also a real person. Our technology is monitored and enhanced by an internal team of scientists who specialize in computer vision, deep learning, and other AI-focused technologies.

Novel attacks are identified, investigated, and triaged in real time and technology enhancements are continuous. This combination of human experts and AI technology is indispensable to harness AI in defending and securing the homeland. But equally important, is the need for AI-based security technologies to be inclusive and uphold privacy mandates by design.

DHS and its component agencies have prioritized transparency and accountability, including performing routine self-assessments and collecting public input on matters of privacy protection and limitations on data use. Those actions serve as a great model for how DHS and other agencies should treat AI capabilities, both in regulating and promoting AI adoption.

The U.S. Government has used biometrics in a growing number of programs over the past decade to improve operational efficiency and traveler experience.

With GenAI, biometrics take on an expanded role of helping to ensure that someone is who they claim to be in digital ecosystems. For example, deep fakes and synthetic identities have recently become so realistic that they are imperceivable to the human eye. Because of this, biometric verification plays a critical role in the Nation's security posture.

To best assist DHS and its components, Congress should support the creation of more useful standards for systems and testing and give access to the best talent developing new technology tools with the agility necessary to respond to the changing threat landscape.

The Silicon Valley Innovation Program is a very powerful model for both acquiring the expertise of the Nation's best engineering minds while also creating a collaborative test bed for providing and proving new technologies. iProov has worked with S&T in all phases of the SVIP program and can testify first-hand to the powerful impact that this program could have if expanded to scale with a broader group of stakeholders.

Another example, the Maryland Biometric Test Facility, could be expanded upon to incorporate a wider range of perspectives as biometric technologies work to address future threats.

In conclusion, we at iProov are completely focused on pioneering capabilities which can counter identity fraud while collaborating with Federal stakeholders to advance innovation. We seek to play a constructive role in AI practices and hope the committee will see us as a resource as you consider a path forward.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Amlani follows:]

Prepared Statement of Ajay Amlani

May 22, 2024

Good morning, Chairman Green, Ranking Member Thompson, and Members of the committee. My name is Ajay Amlani. I've been building innovative solutions to help organizations assure people's identities for the last 20 years. Currently, I serve as the president, head of Americas at iProov.

I started my Federal service as a White House fellow and senior policy advisor to Secretary Tom Ridge, the first Secretary of Homeland Security, in the aftermath of the 9/11 Terrorist Attacks, at a time in which the Federal Government was rethinking how to manage its national security missions, and a large part of that included finding new ways to benefit from the innovation happening in the private sector. For the past 20 years, I have forged partnerships between the Federal Government and the commercial sector that facilitate the utilization of commercial technology to augment national security initiatives. Alongside close colleagues and friends, I have helped to build Government organizations such as DHS and the DoD's Defense Innovation Unit. I have also founded and built commercial technology companies to support Government missions.

Today, this committee is considering how to harness the power of "AI" as part of a multi-layered defense against our adversaries. To best answer this question, we need to start with understanding how AI enables threat actors. What capabilities can DHS and its component agencies develop to combat these threats? What actions can the Department take to better work with industry as it promotes standards for AI adoption?

AI exponentially increases the capabilities and the speed to deploy new fraud and cyber attacks on the homeland. They enable threat technology developers to dramatically shorten their innovation cycles. Ultimately, AI technologies are unique in the way that they "up-skill" threat actors. The actors themselves no longer have to be sophisticated. AI is democratizing the threat landscape by providing any aspiring cyber criminal easy-to-use, advanced tools capable of achieving sophisticated outcomes. The Crime-as-a-Service dark web is very affordable.

The only way to combat AI-based attacks is to harness the power of AI in our cybersecurity strategies. At iProov, we have developed AI-powered biometric solutions to answer a fundamental question: How can we be sure of someone's identity? iProov is trusted by governments and financial institutions globally to combat cyber crime by verifying that an individual is not only the right person, but also a real person. Our technology is monitored and enhanced by an internal team of scientists specialized in computer vision, deep-learning, and other AI-focused technologies. Novel attacks are identified, investigated, and triaged in real-time and technology enhancements are continuous. This combination of human experts and AI technology is indispensable to harness AI in defending and securing the homeland.

But equally important is the need for AI-based security technologies to be inclusive and uphold privacy mandates by design. DHS and its component agencies have prioritized transparency and accountability, including performing routine self-assessments and collecting public input on matters of privacy protection and limitations on data use. I believe those actions serve as a great model for how DHS—and other agencies—should treat AI capabilities in this new wave of Executive action for both regulating and promoting AI adoption.

The U.S. Government has used biometrics in a growing number of programs over the past decade to improve operational efficiency and traveler experience. With

Gen–AI, biometrics take on an expanded role of helping to ensure that someone is who they claim to be in digital ecosystems.

We must emphasize that Gen–AI attack content like deepfakes and synthetic identities have recently become so realistic that it is imperceivable to the human eye. Because of this, I strongly believe that biometric verification must play a critical role in the Nation's security posture. I hope to have the opportunity to expand upon the topic during this hearing.

As iProov thinks about how to best assist DHS and its components, two lines of effort stand out. Those are: (1) Support for the creation of more useful standards for systems and testing; and (2) giving access to the best talent developing new technology tools with the agility necessary to respond to the changing threat environment.

The Silicon Valley Innovation Program (SVIP) performed by DHS's Science and Technology Directorate is a very powerful model for both acquiring the expertise of the Nation's best engineering minds, while also creating a collaborative test bed for proving new technologies. iProov has worked with DHS S&T in all phases of the SVIP program and can testify first-hand to the powerful impact that this program could have if expanded to scale with a broader group of stakeholders.

There is also work occurring inside DHS—like that at DHS S&Ts Maryland Biometric Test Facility—which could be expanded upon to incorporate a wider range of perspectives as biometric technologies work to address future threats.

In conclusion, we at iProov are completely focused on pioneering capabilities which can counter identity fraud, while collaborating with Federal stakeholders to advance innovation. We seek to play a constructive role in AI practices and hope the committee will see us as a resource as you consider a path forward.

Thank you, I look forward to your questions.

Chairman GREEN. Thank you, Mr. Amlani.

I now recognize Mr. Laperruque for 5 minutes to summarize his opening statement.

STATEMENT OF JAKE LAPERRUQUE, DEPUTY DIRECTOR, SECURITY AND SURVEILLANCE PROJECT, THE CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. LAPERRUQUE. Chairman Green, Ranking Member Thompson, and Members of the House Homeland Security Committee, thank you for inviting me to testify on the important topic of artificial intelligence and how we can ensure that its use aids America's national security, as well as our values as a democracy.

I'm Jake Laperruque, deputy director of the Security and Surveillance Project at the Center for Democracy and Technology. CDT is a nonprofit, nonpartisan organization that defends civil rights and civil liberties in the digital age.

We've worked for nearly 3 decades to ensure that rapid technological advances such as AI promote our core values as a democratic society.

AI technology can only provide security if they are used in a responsible manner and, as Chairman Green said, treated with appropriate nuance. This is not only critical for keeping America safe, it is also necessary for protecting our Constitutional values.

Today, I'd like to offer a set of principles for the responsible use of AI, as well as policy recommendations to promote such use in the national security space. We must be worried that for AI technologies garbage in will lead to garbage out. Too often, AI is treated as a sorcerer's stone that can turn lead into gold, but in reality, AI only performs as well as the data that it is given.

Reckless deployment of AI technologies, such as using input data that is low quality or well beyond the bounds of what any given system was designed to analyze, will yield bad results. In the national security space this could have dire consequences, wasted resources, leading investigations astray, or triggering false alarms that leave genuine threats unattended to.

Ensuring that AI is used responsibly is also critical to protecting our values as a democracy. AI is often framed as an arms race, especially in terms of national security, but we must take care of what we're racing toward.

Authoritarian regimes in China, Russia, and Iran have shown how AI technologies such as facial recognition can throttle dissent, oppress marginalized groups, and supercharge surveillance.

The United States must not use AI so callously. Truly winning the AI arms race does not simply mean the fastest build-up on the broadest scale. It requires uses that uphold civil rights and civil liberties. As Ranking Member Thompson highlighted, responsible use requires exercising care from creation to input of data into AI systems to the use of the results from those systems.

To facilitate responsible use, Government applications of AI should be centered on the following principles. AI should be built upon proper training data. It should be subject to independent testing. It should be deployed from the parameters that the technology was designed for.

It should be used by specially-trained staff and corroborated by human review. It should be subject to strong internal governance mechanisms. It should be bound by safeguards to protect Constitutional values. It should be regulated by institutional mechanisms for transparency and oversight.

Although the degree of secrecy in national security programs will make upholding these principles especially challenging, we can and must find ways of promoting responsible use of AI. CDT proposes two policies in furtherance of this goal.

First, Congress should establish an oversight board for the use of AI in national security contexts. This board would be a bipartisan, independent entity within the Executive branch with members and staff given access to all use of AI within the national security sphere.

The board would act as an overseer within Classified settings to promote responsible use of AI so this would support both compliance with existing rules as well as lead to improved practices. The board's role would also allow for greater public knowledge and engagement. This would serve as a conduit for harnessing outside expertise and building public trust in Government's on-going use of AI.

The Privacy and Civil Liberties Oversight Board has demonstrated how effective this model can be. That board's role in counterterrorism oversight has enhanced public awareness and improved public policy in a manner that's aided both security and civil liberties alike. A new board focused on the use of AI in the national security realm would be similarly beneficial.

Second, Congress should enact requirements to enhance transparency for the use of AI. It should include required declassification review of key documents, such as AI impact assessments and privacy impact assessments. It should also require annual public reporting and information such as the full set of AI technologies that agencies deploy, the number of individuals who are impacted by their use, and the nature of that impact.

While we support prompt adoption of these important measures, AI technologies are far too wide-ranging and complex to be solved by a silver bullet. Promoting responsible use of AI will park continual review, engagement, and adaptation. This work should be done in consultation with a broad set of stakeholders, impacted communities, and experts.

Thank you for your time and I look forward to your questions.

[The prepared statement of Mr. Laperruque follows:]

PREPARED STATEMENT OF JAKE LAPERRUQUE

MAY 22, 2024

Chairman Green, Ranking Member Thompson, and Members of the House Homeland Security Committee, thank you for the opportunity to testify on the important topic of how we can ensure that use of artificial intelligence ("AI") enhances America's national security and protects human rights and core democratic values.

I am Jake Laperruque, deputy director of the Security and Surveillance Project at the Center for Democracy & Technology ("CDT"), a nonprofit, nonpartisan organization that defends civil rights, civil liberties, and democratic values in the digital age. For nearly 3 decades, CDT has worked to ensure that rapid technological advances promote our core values as a democratic society.

AI is rapidly altering the world, offering both exhilarating possibilities and alarming risks. It's critical to examine how it should be used in fields where the stakes are highest, such as homeland security. AI can support our goals, but only if we use it properly. While AI capabilities can often prove remarkable, we are wielding complex software systems, not a magic wand. For AI to foster safety and protect our rights, it must be used in a responsible manner. In this testimony I describe key principles for doing so, examine facial recognition as a case study into why responsible use of AI is so critical, and provide a set of steps Congress can take to promote effective use of AI technologies in the national security space.

I. RESPONSIBLE USE AND WELL-DESIGNED SAFEGUARDS ARE ESSENTIAL IF AI IS TO AID NATIONAL SECURITY AND UPHOLD OUR CONSTITUTIONAL VALUES

In order to provide benefits rather than cause harm, AI must be used in a careful and responsible manner. Government use of AI needs at its foundation a set of governance principles, which in turn lead to the development of concrete rules governing AI's acquisition and use. If AI is not developed and deployed responsibly, it will lead our agencies and investigators astray in situations where avoiding errors is most critical. For example, imagine a predictive AI system that was designed to generate leads, but was built on selective or biased training data; such a system will cause investigators to waste time and resources chasing bad leads, leaving genuine security dangers unattended to. Or consider a facial recognition system programmed so poorly that it frequently triggers false alarms, leading investigators not to register the needed level of concern when a real threat appears amid the noise.[1]

In addition to bolstering security, responsible use of AI is critical to upholding our Constitutional values. AI—especially in the context of Government use and national security—is often framed as an "Arms Race." But we must take care in what we're racing toward. Authoritarian regimes in China, Russia, and Iran have all shown how AI can be used to throttle dissent, oppress marginalized groups, and supercharge surveillance.[2] The United States must not recklessly rush ahead with the single-minded goal of deploying AI only to replicate these anti-democratic systems.

[1] See, e.g. Lizzie Dearden, "Facial Recognition Wrongly Identifies Public as Potential Criminals 96 Percent of Time, Figures Reveal", *The Independent,* May 7, 2019, *https://perma.cc/YZ36-RC6A.*

[2] Paul Mozur, "In Hong Kong Protests, Faces Become Weapons", *N.Y. Times,* July 26, 2019, *https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html;* Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", *N.Y. Times,* Apr. 14, 2019, *https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html;* Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *N.Y. Times,* July 8, 2018, *https://perma.cc/27U7-S365;* Lena Masri, "Facial Recognition is Helping Putin Curb Dissent With the Aid of U.S. Tech", *Reuters,* Mar. 28, 2023, *https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/;* Khari Johnson, "Iran to Use Facial Recognition to Identify Women Without Hijabs", *Ars Technica,* Jan. 11, 2023, *https://arstechnica.com/tech-policy/2023/01/iran-to-use-facial-recognition-to-identify-women-without-hijabs/.*

Truly winning the "AI Arms Race" does not mean simply achieving the fastest build-up on the broadest scale. It requires deployment in a manner that reflects and advances America's Constitutional values.

We are at a time of public anxiety and uncertainty about AI. Securing the trust of the American people and our global allies—as well as maintaining an advantage over adversaries—can only be achieved if we demonstrate that this technology will both be effective and support civil rights, civil liberties, and democratic values.

II. PRINCIPLES FOR ENSURING RESPONSIBLE USE OF AI TECHNOLOGIES

The Department of Homeland Security ("DHS") has taken a positive step in highlighting the need for responsible use of AI in its recently-published AI Roadmap, and offering principles for doing so.[3] Notably, the Roadmap commits to its use of AI being "rigorously tested," "safeguard[ing] privacy, civil rights, and civil liberties," and being "transparent and explainable." It is critical that DHS and other Government agencies that use AI for national security purposes adhere to and build upon these and other key principles.

Principles for responsible use of AI technologies should be applied broadly across development and deployment. In particular, Government use of AI should be:

(1) Built upon proper training data;
(2) Subject to independent testing and high performance standards;
(3) Deployed only within the bounds of the technology's designed function;
(4) Used exclusively by trained staff and corroborated by human review;
(5) Subject to internal governance mechanisms that define and promote responsible use;
(6) Bound by safeguards to protect human rights and Constitutional values; and
(7) Regulated by institutional mechanisms for ensuring transparency and oversight.

Training Data.—Proper training data is the first hurdle to avoiding "garbage in, garbage out" problems with AI. The effectiveness of AI systems depends on the data used to develop them. If data is inaccurate or of poor quality, then the resulting system trained from it will exhibit flaws. Training data does not even need to be wrong to cause problems—training AI on selective and unrepresentative data can warp how those AI systems later function. For example, a common flaw discovered in facial recognition systems was use of training sets that were disproportionately white and male; as a result these systems displayed algorithmic bias in which women and people of color were misidentified at far higher rates.[4]

Independent Testing.—Requiring independent testing and high performance standards is a key safeguard against adoption of low-quality systems. Such measures are important because poor algorithm design or flawed training data are not always readily apparent, and AI technologies are frequently being applied to new situations and circumstances. Testing should be conducted by independent experts, with transparent methodology that allows for peer review and improvement. Testing should occur periodically, and should be a precondition for procurement, as well as regularly conducted for AI systems already in use. And critically, systems should be tested in real-world contexts (e.g., in pilots or limited releases), using the same system settings as will be used in actual deployments, and using real-world scenarios. As those system settings or scenarios change or evolve, testing should evolve to account for them.

Deploy Only for Designed Function.—Deploying AI technologies only within the bounds of the technology's designed functions is a principle that takes on several components. This requires making sure that "input data"—meaning the data and requests that AI technologies analyze and base their outputs on—is proper. It must be high-quality, which can be challenging as input data often exists on a sliding scale and depends upon a huge range of factors, and cannot simply be labeled "good data, use it" or "bad data, toss it." For example, as discussed in detail below, a wide range of factors impact whether an image can be effectively scanned by facial recognition technology.[5]

[3] Dept. of Homeland Security, Artificial Intelligence Roadmap 2024 (2024), *https://perma.cc/Y6KQ-5J9V.*

[4] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Fairness, Accountability and Transparency,* Proceedings of Machine Learning Research 81:77–91 (2018), *https://perma.cc/C9FV-G5SY;* Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects,* National Institute of Standards and Technology (2019), *https://doi.org/10.6028/NIST.IR.8280.*

[5] See Section III.

Assessing whether certain data and tasks properly fit within an AI technology's designed capabilities can also be hard to discern. For example, as CDT has discussed, automated social media analysis tools can be undone when tasked with reviewing posts that contain slang, sarcasm, and other context-specific language.[6] AI can also be deployed egregiously beyond the bounds of the technology's designed functions. It is critical that the Government not treat AI technologies as a philosopher's stone that can turn lead into gold—if a system is tasked with analyzing poor-quality data or given tasks beyond its designed function, it will produce unreliable results.

Training and Human Review.—The often challenging nature of evaluating the proper bounds for using an AI technology highlight why training and human review is another essential principle. If staff using AI are not specifically trained in how it should be deployed, poor results will follow. Training is also necessary for preventing automation bias—meaning the tendency for people to naturally assume automated systems are correct, even in the face of conflicting evidence—in general, and in particular for effectively gauging how much weight to give results from AI in various situations. And even when AI is used in the most favorable settings, accuracy cannot be guaranteed, making human review and corroboration of results essential. Human review is important not only to account for naturally-occurring errors in AI systems, but also to guard against risk of malicious tampering that degrades results.[7] Further, human approval should be required before AI systems are used to take specific actions that may affect individuals' rights (e.g., targeting a person for surveillance).

Internal Governance.—Agencies should put in place internal governance mechanisms to promote responsible use of AI. The recently-released Office of Management and Budget's (OMB) guidance on governance and risk management for Federal agencies' use of AI is an important step forward in advancing this goal.[8] That OMB memo should serve as a baseline for the forthcoming National Security Memorandum that is intended to establish parallel guidance for national security systems. The OMB guidance provides useful direction to agencies concerning internal governance processes in support of responsible and transparent use of AI technologies. Agencies should clearly assign decision-making and internal oversight responsibilities, including requirements for approval by high-level officials for procurement of systems and use cases that present particularly high risks. Legal, civil rights, and privacy officials should be part of the decision-making process through the AI development, procurement, and deployment life cycle and have comprehensive visibility into how departments and agencies are using AI.

Effective governance also requires clear standards for procurement of AI technologies from third-party vendors.[9] Standards should include requirements for pre-award Government evaluation of vendors' AI models to reject vendors whose models don't address the needs agencies identify.[10] Standards should also include contractual requirements for vendor reporting with sufficient detail to support agencies' ongoing independent review of model performance, evaluation of and reporting on impacts, and agencies' own disclosures in their AI inventories.[11]

Safeguarding Rights.—While the principles above largely focus on ensuring AI is as accurate and efficacious as possible, it is also essential that AI technologies are used in a manner that upholds Constitutional values, civil rights, and civil liberties. Safeguards for achieving this cannot merely consist of generally tasking agencies or individual staff with abiding by broad principles, and hoping that AI's use will be properly restrained on a case-by-case basis.

Agencies should conduct impact assessments to determine whether an AI system risks being biased or otherwise violating Constitutional and human rights. Certain AI technologies or uses should be prohibited because they pose an unacceptable risk to rights (e.g., AI profiling or risk scoring systems that attempt to predict an indi-

[6] Mana Azarmi, "The U.S. Government is Demanding Social Media Information From 14.7 Million Visa Applicants—Congress Should Step In", Center for Democracy & Technology, Jul. 3, 2019, *https://perma.cc/JMK8-BA7B.*

[7] See Section V.

[8] Office of Management and Budget, *M–24–10: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (Mar. 28, 2024), *https://perma.cc/RKK7-SMYJ.* See also, Center for Democracy & Technology, "CDT Welcomes Final OMB Guidance on Federal Agencies' Use of AI, and Now Looks Toward Earnest Implementation", Mar. 28, 2024, *https://perma.cc/MQ34-VUWG.*

[9] Hannah Quay-de la Vallee et al, Center for Democracy & Technology, *The Federal Government's Power of the Purse: Enacting Procurement Policies and Practices to Support Responsible AI Use* (2024), *https://perma.cc/BL2L-5Z6M.*

[10] Id. at 37–39.

[11] Id. at 39–40, 42–45.

vidual's future criminality). As the OMB memorandum notes, "[w]here the AI's risks to rights or safety exceed an acceptable level and where mitigation is not practicable, agencies must stop using the affected AI as soon as practicable." In cases where a system poses risks that can be mitigated, agencies should impose specific and concrete rules tailored to each specific AI technology and its use scenarios. For example, agency guidelines on use of facial recognition should account for image quality in various ways, and strictly regulate what (if any) adjustments may be made to an image prior to scanning. Agency rules must be designed to promote both efficacy and protection of civil rights, civil liberties, and Constitutional principles. While agency rules are an essential first step, Congress should also bolster protections with statutory safeguards as needed for AI technologies that present significant risks to civil rights and civil liberties.

Transparency & Oversight.—Upholding responsible use will require mechanisms for transparency, oversight, and accountability. Such efforts must be institutionalized systems, rather than ad hoc review. Oversight structures should exist within agencies, and across the Federal Government. Systems should also be designed to facilitate public review and input, which is important for fostering trust, ensuring compliance with rules, and promoting improvements in how AI technologies are used. This will be challenging in terms of use of AI in national security spheres where secrecy is the norm, but this cannot be an excuse for inaction. Section IV of this testimony proposes certain measures Congress could take that are specifically designed to account for the secrecy of national security operations while promoting public engagement.

III. FACIAL RECOGNITION AS A CASE STUDY OF WHY RESPONSIBLE USE IS KEY FOR BOTH SECURITY AND DEMOCRATIC VALUES

Facial recognition serves as a premiere example of why responsible use of AI technologies is critical to ensuring safety as well as civil rights and civil liberties, and why the principles described above serve as the foundation for responsible use. Facial recognition is especially fitting in evaluating responsible use because it is an AI technology that the Government has used for law enforcement and security purposes for roughly a decade.[12] Facial recognition can provide a road map of why key principles are essential, as well as offer clear warnings about how irresponsible and careless uses undermine public safety.

AI technologies are too often viewed more as magic than software. This problem has occurred in practice with facial recognition, which is sometimes treated as universally applicable and virtually infallible. For example, major facial recognition vendors have reportedly included marketing materials and user instructions that improperly claim the technology won't produce false matches, will provide definitive identifications rather than candidate lists, and can be used on low-quality images without impairing results.[13] Clearview AI—which, despite its notoriety, is used by 10 Federal law enforcement entities including Customs and Border Protection and

[12] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America,* Georgetown Law Center on Privacy and Technology, Oct. 18, 2016, *https://www.perpetuallineup.org/*.

[13] Jake Laperruque, "Key Facts About Face Recognition for Policymaking", Project on Government Oversight, Aug. 24, 2021, *https://perma.cc/VBW6-Q44G*. ("Tech Vendors' Exaggerations About How Face Recognition Functions: Claim: According to Clearview AI, "you will almost never get a false positive. You will either get a correct match or nor [sic] results." Fact: Any system, no matter how advanced its algorithm, can produce false positives. Claim: FaceFirst stated, "Facial recognition gives officers the power to instantly identify suspects . . . " " . . . Officers can simply use their mobile phones to snap a photograph of a suspect from a safe distance. If that individual is in their database it can then positively identify that person in seconds with a high degree of accuracy." Fact: Field conditions for this scenario—such as lighting, angle, and distance—significantly increase the likelihood of misidentifications. Claim: DataWorks Plus pitched its systems as tech that "uses facial recognition technology to positively match photos of an individual" with capabilities such as "discovering a person's identity during investigations." Fact: Face recognition can offer sets of possible matches, but should not be relied on to offer a definitive, positive match. Claim: Matches with low confidence thresholds can be acceptable. Amazon worked with police to develop a system that will always "return the top 5 leads based on confidence levels" (meaning the Amazon-recommended setting will return matches no matter how low the confidence threshold is) and touted the fact that police are "willing to trade a lower confidence level for more leads." Fact: Using an unrestricted setting that always returns matches—no matter how low the confidence threshold—creates serious risk of misidentifications. Claim: Clearview AI said, "A photo should work even if the suspect grows a beard, wears glasses, or appears in bad lighting." Fact: Photo conditions that limit ability to scan facial features impact the ability to accurately obtain matches. Obstructions and low lighting make misidentifications more likely even for high-performing systems".

Immigration and Customs Enforcement[14]—went so far as to post advertisements to police networks claiming that law enforcement officials would "realize you were the crazy one" for not expecting face recognition to function the same as in absurd TV depictions like "NCIS, CSI, Blue Bloods."[15] These claims are not just untrue; they encourage law enforcement to engage in unsafe practices and build investigations around unreliable, low-quality marches.

In reality, facial recognition's effectiveness is highly variable, and depends upon a range of factors. First, the reliability of facial recognition depends upon the quality of images being scanned; images with low lighting, bad resolution, poor angles, or obstructions are much less likely to yield reliable matches.[16] This is a prime example of how AI is only as good as the data it interacts with. There is no clear line that separates "good usable images" and "bad unusable images" into two neat groups. Rather, there is a gradation based on all the image-quality factors listed above, each of which has a huge range; evaluating how much value to give to matches from photos across that range can be highly difficult.

Accuracy of facial recognition is also impacted by the significant variance in how effective different facial recognition systems are based on factors such as overall quality of the training data, as well as degree of algorithmic bias. While some systems claim to have overcome demographic variance in accuracy, for others it is a huge problem; a National Institute of Science and Technology study found certain systems were up to 100 times more likely to misidentify Asian and African American people than white men.[17] Low-quality training data—in particular, using databases of faces that are demographically skewed—is the main source of this problem.[18]

System settings impact the quality of results as well. Many law enforcement entities, including the FBI, configure systems to always return a set of potential matches for a facial recognition scan, no matter how reliable (or unreliable) those matches are.[19] Such practices inevitably yield matches that are undependable, but might be interpreted as a credible lead from highly-sophisticated AI technology.

Furthermore, it is disturbingly common for law enforcement to artificially replace portions of faces they are scanning; this practice injects further uncertainty and speculation into results.[20] Techniques for doing so range from using computer-generated imagery (CGI) to add pieces of a face not captured in photos, to replacing the real face entirely with a composite sketch or celebrity look-alike.[21] This conduct

[14] Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks,* GAO–21–518, at 12 (2021), *https://www.gao.gov/assets/gao-21-518.pdf;* see also Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties,* GAO–23–105607, *https://www.gao.gov/assets/gao-23-105607.pdf* (describing continued use of Clearview by at least 6 agencies).

[15] Jake Laperruque, "Correcting Misconceptions and Planning Effective Safeguards on Face Recognition Technology", Project on Government Oversight, Jul. 13, 2021, *https://perma.cc/S7TT-Z85Z.*

[16] See, Artificial Intelligence and Human Rights: Hearing Before the Sen. Subcomm. on Human Rights and the Law of the Sen. Comm. on the Jud., 118th Cong. (2023) (testimony of Alexandra Reeve Givens, president and CEO, Center for Democracy & Technology), *https://perma.cc/5ZKF-J97B;* see also, The Constitution Project's Task Force on Facial Recognition Surveillance and Jake Laperruque, "Facing the Future of Surveillance", Project on Government Oversight, Mar. 4, 2019, *https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance.*

[17] Drew Harwell, "Federal Study Confirms Racial Bias of Many Facial-Recognition Systems, Casts Doubts on Their Expanding Use", *Washington Post* (Dec. 19, 2019), *https://perma.cc/8RJE-VBMH.*

[18] See, "Joy Buolamwini: How Does Facial Recognition Software See Skin Color?", National Public Radio: TED Radio Hour, Jan. 26, 2018, *https://www.npr.org/transcripts/580619086;* see also Joy Buolamwini, "Unmasking the Bias in Facial Recognition Algorithms", MIT Sloan School of Management, Dec. 13, 2023, *https://perma.cc/7J6P-JDG4.*

[19] See, Erin M. Priest, Privacy and Civil Liberties Officer, FBI, "Privacy Impact Assessment for the Next Generation Identification-InterState Photo System," (2019), *https://perma.cc/FR82-SFPB* ("A gallery of two to fifty photos will be returned, with the law enforcement agency choosing the size of the gallery. If no choice is made, a default of 20 photos is returned").

[20] Clare Garvie, "Garbage In, Garbage Out/Face Recognition on Flawed Data", Georgetown Law Center on Privacy & Technology, May 16, 2019, *https://perma.cc/D4BL-WQGU.*

[21] James O'Neill, "How Facial Recognition Makes You Safer", *N.Y. Times,* June 9, 2019, *https://www.nytimes.com/2019/06/09/opinion/facial-recognition-police-new-york-city.html* ("We have used editing software to substitute a generic feature when a suspect is closing his eyes or sticking out his tongue in the submitted photo. The system can also create a mirror image of the right side of a face if we have only the left side, for example, to produce a 3–D model"); Clare Garvie, "Garbage In, Garbage Out/Face Recognition on Flawed Data", Georgetown Law Center on Privacy & Technology, May 16, 2019, *https://perma.cc/D4BL-WQGU* ("One detective from the Facial Identification Section (FIS), responsible for conducting face recognition

puts the veneer of useful intel built from objective, high-tech tools onto shoddy and baseless results.

All of these factors demonstrate the need for rigorous guardrails on the design and use of face recognition technology. We have already seen the devastating effect that lax practices and overreliance on facial recognition can have on people's rights, with misidentifications that led to wrongful arrests, and jail time for innocent individuals.[22] Beyond the undue deprivation of liberty, these errors have caused lasting harms including loss of employment, enormous legal bills, and mental health issues.[23] Unfortunately, because the role of facial recognition investigations is often hidden, these incidents are likely just several among many instances in which poor applications of the technology have caused wrongful arrests.[24] [25] Beyond the significant harm to the individuals improperly flagged as matches, reliance on facial recognition errors undermines public safety by leading investigations far afield, which could have especially severe consequences in the national security context.

Facial recognition also gives a dire warning to why responsible use is necessary to protect Constitutional values. Absent strong safeguards, AI can supercharge anti-democratic practices, and severely harm civil rights and civil liberties. In China, facial recognition is used for surveillance on a mass scale, including to oppress the nation's Uyghur populace.[26] The pervasive application of facial recognition in itself becomes a means for authoritarianism: By using facial recognition for low-level offenses such as jaywalking, the Chinese government creates a digital panopticon, threatening its people with the fear that the government, empowered by AI, is always watching.[27] The governments in Russia and Iran also weaponize facial recognition to thwart dissent, with Russia deploying the technology against anti-war protesters and Iran using it to identify and threaten those demonstrating against the state's hijab mandate.[28]

Yet these disturbing and improper uses have not just occurred abroad—in the United States there are already documented instances of facial recognition being deployed against peaceful protesters.[29] This and other anti-democratic uses must not

searches for the NYPD, noted that the suspect looked like the actor Woody Harrelson . . . A Google image search for the actor predictably returned high-quality images, which detectives then submitted to the face recognition algorithm in place of the suspect's photo.")

[22] See, Khari Johnson, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives", *Wired,* Mar. 7, 2022, *https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/;* Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", *N.Y. Times,* Dec. 29, 2020, *https://perma.cc/CHM4-QAZ3;* Kashmir Hill and Ryan Mac, "'Thousands of Dollars for Something I Didn't Do,'" *N.Y. Times,* Mar. 31, 2023, *https://perma.cc/CNK3-926N;* Johana Bhuiyan, "Facial Recognition Used After Sunglass Hut Robbery Led to Man's Wrongful Jailing, Says Suit," *Guardian,* January 22, 2024. *https://www.theguardian.com/technology/2024/jan/22/sunglass-hut-facial-recognition-wrongful-arrest-lawsuit.*

[23] See, Khari Johnson, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives", *Wired,* Mar. 7, 2022, *https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/;* Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match", *N.Y. Times,* Dec. 29, 2020, *https://perma.cc/CHM4-QAZ3;* Kashmir Hill and Ryan Mac, "'Thousands of Dollars for Something I Didn't Do,'" *N.Y. Times,* Mar. 31, 2023, *https://perma.cc/CNK3-926N.*

[24] Khari Johnson, "The Hidden Role of Facial Recognition Tech in Many Arrests", *Wired,* Mar. 7, 2022, *https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/;* Jennifer Valentino-DeVries, "How the Police Use Facial Recognition, and Where it Falls Short", *N.Y. Times,* Jan. 12, 2020, *https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html.*

[25] Disturbingly, it is likely that facial recognition misidentifications have caused innocent individuals not just to temporarily be held in jail but to actually face prison sentences, with charges based on erroneous matches leading to either wrongful conviction or accepting a plea bargain out of fear of long sentences or extended time in pretrial detention.

[26] Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", *N.Y. Times,* Apr. 14, 2019, *https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html;* Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *N.Y. Times,* July 8, 2018, *https://perma.cc/27U7-S365.*

[27] Alfred Ng, "How China Uses Facial Recognition to Control Human Behavior", CNET, Aug. 11, 2020, *https://perma.cc/P6Y3-U7XV* ("The punishing of these minor offenses is by design, surveillance experts said. The threat of public humiliation through facial recognition helps Chinese officials direct over a billion people toward what it considers acceptable behavior, from what you wear to how you cross the street").

[28] Lena Masri, "Facial Recognition is Helping Putin Curb Dissent With the Aid of U.S. Tech", Reuters, Mar. 28, 2023, *https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/;* Khari Johnson, "Iran to Use Facial Recognition to Identify Women Without Hijabs," *Ars Technica,* Jan. 11, 2023, *https://arstechnica.com/tech-policy/2023/01/iran-to-use-facial-recognition-to-identify-women-without-hijabs/.*

[29] Joanne Cavanaugh Simpson and Marc Freeman, "South Florida Police Quietly Ran Facial Recognition Scans to Identify Peaceful Protestors. Is That Legal?", *Sun Sentinel,* June 26, 2021,

Continued

become the norm. Strong rules must be put into place to protect civil rights and civil liberties.[30]

Even though law enforcement use of face recognition is too often cloaked in secrecy, we at least know about the existence of this technology and have some insights into how Government deploys it, and public interest researchers have been able to test and critique it. Unfortunately this is not the case with other AI products that may be in use. We do not have a broad list of AI technologies deployed in the national security space, let alone details on use that would allow us to effectively evaluate efficacy and risks. That is why it is essential that Congress consider the appropriate institutional mechanisms for ensuring transparency, oversight, and accountability.

IV. CONGRESS SHOULD ESTABLISH INSTITUTIONAL OVERSIGHT MEASURES TO SUPPORT RESPONSIBLE USE

Given its complexity and the range of technologies AI consists of, there will be no silver bullet for ensuring responsible use and adherence to the key principles outlined in this testimony. Instead, we should attempt to develop and continuously build on a broad set of policies that promote transparency, oversight, and accountability at a broad level, while vigorously working to enact and enforce specific regulations for each AI technology tailored to maximize its efficacy and adherence to democratic principles. In its recent AI Roadmap, DHS noted that responsible use of AI requires "continuous monitoring to build trust and accountability in AI applications," and the agency committed to establishing "safe, secure, and trustworthy use of AI by DHS through robust governance and oversight policies and practices."[31]

Congress should take steps in support of that goal through the measures discussed below. While these policies are important and we support their prompt adoption, they should not be viewed as comprehensive solutions. Promoting responsible use of AI will require continual engagement, review, and adaptation; this work must be done in consultation with a broad set of experts, impacted communities, and other stakeholders.

a. Oversight Board for Use of AI and National Security

Development and enforcement of proper policies for responsible use of AI is especially challenging in the national security space because Government operations in this realm are often shrouded in secrecy. Active investigations, tradecraft, and protection of sources and methods limit public knowledge. The level of secrecy due to these legitimate factors is compounded by overclassification.

As a flagship tool for ensuring responsible use in the face of this obstacle, Congress should create an oversight board for the use of AI in national security, modeled after the Privacy and Civil Liberties Board ("PCLOB"), established by the 9/11 Commission Act of 2007. This AI Oversight Board would be a bipartisan, independent entity within the Executive branch, with members and staff possessing security clearances and given access to all use of AI within the national security sphere. The AI Oversight Board would be tasked with:

(1) Serving as an overseer within Classified settings to promote responsible use of AI. Such work would involve not only fostering compliance with existing rules, but also encouraging improved agency practices.

(2) Facilitating greater public knowledge and understanding of uses of AI in the national security space, through development of reports and seeking viable declassification of relevant documents and information. In this work the AI Oversight Board should also solicit input of outside experts, affected communities, and other stakeholders. This would help building public trust, and serve as a conduit for outside expertise to improve use of AI in the national security space.

(3) Provide policy recommendations to both the administration and Congress to better ensure that use of AI is responsible, aids security, and advances democratic values.

PCLOB demonstrates how effective this model can be for balancing the need for oversight with the secrecy built into national security space. Over the past 15 years, PCLOB has proven highly valuable in increasing public knowledge in the counterterrorism space, and thereby promoting better public policy for both security and civil liberties. For example, in 2014 PCLOB's report on use of the PATRIOT Act to

https://www.sun-sentinel.com/2021/06/26/south-florida-police-quietly-ran-facial-recognition-scans-to-identify-peaceful-protestors-is-that-legal/.

[30] CDT has previously advanced a number of policy proposals to accomplish this goal, which we described in Section IV(d).

[31] Dept. of Homeland Security, *Artificial Intelligence Roadmap 2024,* at 15–16 (2024), *https://perma.cc/Y6KQ-5J9V.*

conduct bulk collection of Americans' phone records demonstrated that despite its massive privacy harms, the program did not provide any meaningful counterterrorism value as its proponents had claimed.[32] This thorough and independent assessment of the program's efficacy was invaluable to the public debate over the bulk collection program, which Congress chose to outlaw the following year.[33]

PCLOB has also been greatly useful in relation to Section 702 of the Foreign Intelligence Surveillance Act. PCLOB has issued multiple reports on this warrantless surveillance authority, resulting in declassification of hundreds of pieces of information about the program, helping explain how certain operations under the law function, providing insights into the effectiveness and risks of various activities, and included over a dozen policy recommendations.[34] This work had a significant positive impact on the recent public debate over Section 702's reauthorization that occurred over the past year.

We urge Congress to promptly establish an oversight board for use of AI in national security modeled after PCLOB in its structure, access to information, and obligations. And although we believe PCLOB provides an insightful road map, we also recommend Congress consult with PCLOB and other stakeholders on what institutional features could be adjusted to improve this new AI Oversight Board's effectiveness, as well as what distinctions might be necessary to better support its focus on AI.

b. Robust Transparency and Reporting Structure

While internal agency rules are necessary, they are far from sufficient to ensure responsible use of AI, especially given the secrecy of national security activities. Transparency and public awareness are a baseline for maintaining compliance by agencies and continued improvements in policy. The AI Oversight Board discussed above will contribute to this goal, but should not be laden with the full responsibility for achieving it. Congress should build institutionalized transparency and reporting structures into Government use of AI for national security in at least two ways.

First, Congress should require declassification review of key documents on use of AI for national security. This should include all AI Impact Assessments, as well as Privacy Impact Assessments, Human Rights Impact Assessments, or Privacy Threshold Analyses conducted in relation to AI technologies. Required declassification review should also apply to agency guidelines for use of AI technologies, and legal analyses regarding use of AI systems. Finally, it should include any efficacy assessments of AI systems. Following the model of required declassification review for significant FISA Court opinions that Congress enacted as part of the USA FREEDOM Act in 2015, reviews should be conducted in a timely manner, and, if significant redactions that might impair understanding of the document are included, be accompanied by an unclassified summary.

Second, Congress should require annual agency reporting on use of AI technologies. These reports should include information describing: (1) The type of AI technologies used; (2) the types of data being analyzed by each AI technology used; (3) the types of Government activities each AI technology is used for; (4) the number of individuals impacted by AI technologies and nature of that impact; and (5) the number of criminal, immigration, and administrative court proceedings in which evidence obtained or derived from AI technologies was submitted into evidence. The Office of the Director of National Intelligence Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities—composed largely of data Congress required be reported annually as part of the USA FREEDOM Act—could be instructive in developing these annual reports on use of AI technologies, especially as they are used in the national security context.

c. Build Institutional Mechanisms Into Funding

Given the pace of development and the stakes of this issue, the Government must not deploy AI technologies now and plan to develop best practices and sort through

[32] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (2014), *https://perma.cc/HS93-J5U3.*

[33] See, Center for Democracy & Technology, "Victory: Passage of USA FREEDOM Act Reins in NSA Surveillance", Jun. 2, 2015, *https://perma.cc/K6BC-X96A.*

[34] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2023), *https://perma.cc/M73R-ZK4D;* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2014), *https://perma.cc/S5KV-88GL.*

mistakes later. As Congress considers upcoming funding for new applications of AI in the national security realm, it should require that agencies adopt institutional mechanisms such as those described above as part of their governance of AI development and deployment. If Congress does not take such steps now, we may find ourselves too far behind to keep up with developments and ensure responsible use.

d. Establish statutory safeguards for the most rights-impacting AI technologies

While agencies should institute impact assessments and internal guidelines to protect civil rights and civil liberties, Congress should also supplement these rules with statutory protections, particularly for AI technologies that pose the most significant risks to individual rights. Self-policing often proves insufficient for protecting civil rights and civil liberties in the national security context. And even where internal guidelines are ideal, independent checks and safeguards are needed to ensure that limits cannot be rolled back by the very agency governed by them. As more information about specific AI uses is revealed, it will be necessary for Congress to step in for those AI technologies that have the greatest potential to impact rights, codify agency rules that are effective, and establish additional safeguards as necessary. For example, CDT has previously issued a set of key policy recommendations for facial recognition centered on: (1) warrants, (2) a serious crime limit, (3) disclosure to arrested individuals, (4) testing and accuracy standards, and (5) limiting the degree of reliance on matches for law enforcement activities.[35] Those rules are critical given the specific risks facial recognition poses, and were crafted to account for how best to protect civil rights and civil liberties while also maximizing efficacy given particular uses of that technology. Congress should work to develop and implement properly tailored rules for other AI technologies that are especially rights-impacting as we obtain greater knowledge on their use.

V. CAREFUL EVALUATION OF AI IS KEY TO DEFENDING AGAINST MODERN THREATS

As Congress evaluates Government use of AI in the national security space and proper safeguards, it is also important to consider how understanding and preparing for use of AI is necessary to defend against modern threats to security. This vigilance will be necessary in a variety of spheres.

Congress should rigorously examine use of AI within critical infrastructure. Malicious tampering with AI systems deployed in critical infrastructure could have disastrous implications for national security, especially because the dangerous outputs from such tampered systems might not be readily apparent. These risks are just as present for AI applications in critical infrastructure that are entirely disconnected from security operations (such as an automated system for tracking power usage and distributing energy availability) as those built specifically for it (such as facial recognition systems at airports).[36]

We should also be wary how adversaries might harness AI to augment long-standing attack threats, such as in terms of cybersecurity.[37] Bad actors will use AI to augment the scale of attacks, such as having AI technologies help write and augment software deployed in malicious hacking efforts. AI can also provide new weapons in furtherance of more traditional hacking methods. For example a dedicated spear-phishing attack previously conducted via an email or text message could in the future be accompanied by a deep fake voice or video message to increase the odds of deceiving a target. AI itself may prove useful to mitigating these threats—a variety of technological advances have been applied in cybersecurity settings to tip the balance back and forth between attackers and defenders. We should be vigilant in identifying AI-based cybersecurity threats and swift in responding to them, but must also consistently adhere to principles for responsible use of AI, even as a countermeasure to emerging threats. Doing so is the only way to ensure these responses are effective.

Election security is another area where AI technologies may present risks. Generative AI could be used to create convincing fake election records, or produce FOIA

[35] See, Artificial Intelligence and Human Rights: Hearing Before the Sen. Subcomm. on Human Rights and the Law of the Sen. Comm. on the Jud., 118th Cong. (2023) (testimony of Alexandra Reeve Givens, president and CEO, Center for Democracy & Technology), *https://perma.cc/5ZKF-J97B.*

[36] See, Dept. of Homeland Security, *Artificial Intelligence Roadmap 2024,* at 6 (2024), *https://perma.cc/Y6KQ-5J9V* ("Generating and passing poisoned data into a critical sensor could trigger downstream impacts, such as service disruptions or system shut-offs").

[37] As DHS highlights in its recently published AI Roadmap, "The proliferation of accessible AI tools likely will bolster our adversaries' tactics. Cyber actors use AI to develop new tools that allow them to access and compromise more victims and enable larger-scale cyber-attacks that are faster, more efficient, and more evasive." Id.

requests at a mass scale designed to overwhelm election officials.[38] AI technologies not only expand the range of possible malicious activities, they make misconduct feasible at a larger scale and lower costs. The decentralized nature of our election system adds to the challenge of defending this space. Federal agencies already coordinate information on cybersecurity risks across thousands of election jurisdictions as they emerge through the Election Infrastructure Information Sharing and Analysis Center, provide funding through election security grants, support election officials and administrators, and assist in educating the public about where to find accurate information about elections. Actors in this space should also identify and account for AI-based threats as they emerge. Additionally, while Federal agencies' application of AI in the elections space is limited, they should provide oversight and guidance on the use of these tools to State and local election administrators.[39]

CONCLUSION

While the scope and capabilities of AI technologies may be daunting, executive agencies and Congress should treat it with the same careful consideration as any other powerful machine. Safety, security, and promotion of democratic values can only stem from responsible use. Achieving this requires adherence to principles such as those described above, and Congress has a key role in establishing the oversight and transparency mechanisms that will advance those principles. If we rush to deploy AI quickly rather than carefully, it will harm security and civil liberties alike. But if we establish a strong foundation now for responsible use, we can reap benefits well into the future.

Chairman GREEN. Thank you, sir.

Members will be recognized by order of seniority for their 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized.

I now recognize myself for 5 minutes of questioning. Mr. Amlani, in the evolution of AI would you discuss your perception or opinion on whether or not you think as the threat evolves we are evolving ahead of the threat?

Mr. AMLANI. Thank you, Mr. Chairman, for the question. This is a very important component of the work that we do at iProov. At iProov we have a central operations center where we monitor all the threats happening globally. We have deployments worldwide, Singapore, United Kingdom, Australia, Latin America, Africa, and the United States, and we're constantly using our human people there with PhDs to be able to assess the threats that are actually trying to attack biometric systems globally.

We're migrating and adapting our AI technology to stay multiple steps ahead of the adversary, and I think this is very critical as we look at AI technology to be able to build in steps to continue to stay multiple steps ahead of the adversaries and understanding what attacks are actually happening globally so that we can continue to modify our systems.

Chairman GREEN. Well, thank you for that. I am glad to hear that. I think it makes everybody sigh a little bit relief, but, you know, I want to shift the subject a little bit because we are talking about AI as a tool and as a, you know, all the positives and then the challenges of it when it is on the attack side. But I want to ask something about work force.

[38] See Tim Harper, "CDT Hosts Roundtable on Generative AI and Elections with U.S. Department of State Bureau of Cyberspace and Digital Policy", Center for Democracy & Technology, Mar. 13, 2024, *https://perma.cc/5Q9A-J7GJ.*

[39] While generative AI has yet to be adopted in any meaningful way by election officials, non-generative AI has been introduced into election administration in recent years. Some election offices have used AI-powered software for administrative purposes including matching mail-in ballot signatures or translating voting materials. See Edgardo Cortés et al, *Safeguards for Using Artificial Intelligence in Election Administration,* Brennan Center for Justice (2023), *https://perma.cc/86VR-A82A.*

You know, what do we need to do uniquely and this, Mr. Sikorski, would really I think be for you since, you know, your company employs a very large number of individuals in this fight, you know, how do we need to be thinking about developing the work force for AI as well as cybersecurity in itself?

Mr. SIKORSKI. Yes, that's a great question, Congressman. I think it's super imperative. Myself I've trained cyber agents for the FBI at Quantico, Department of Energy employees, private companies, and then I've been teaching at the university level for over a decade.

First-hand I've seen that we really need to focus in as AI cybersecurity, it's here to stay, and we need to really make strides to continue to push down, get people trained up, our work force, our children get them learning these concepts very early on is super important.

Then from a Palo Alto Networks perspective, we're very invested in this as well. So as far as the Unit 42 team goes within Palo Alto Networks we have what's called the Unit 42 Academy which takes undergraduates, give them internships during the college years, hands-on training.

Then they come to work with us as a class, like a cohort, where they learn a lot of up-leveling skills and their first year is spent just engaged in learning and growing. I'm proud to say that 80 percent of the Unit 42 Academy in the last year was actually made up of women.

Chairman GREEN. Do me a favor and let's go just a little bit more granular on this question. What are the skills, specific skills, that these individuals need to have? What are we teaching them? I get, you know, the coding and all that stuff, but what specifically do you need to see in a candidate that you would want to hire?

Mr. SIKORSKI. Yes, so No. 1 is having a background and understanding how to engage these technologies. We've spent a lot of time building technologies over the last 10, 20 years in the cybersecurity industry, so knowledge of how they work, what they give them access to, and how they can leverage them to fight against, you know, evil that's coming into these networks.

I also think about things like understanding of how computer forensics works, malware analysis, an ability to really dive deep into the technical details so that they could dig out and sift through the noise. That also comes into play with AI.

Do they have an understanding of AI and how it is being leveraged in the product to sift through that noise for them? Because one thing we deal with heavily is these analysts are inundated with just too many alerts from all these products firing and in those alerts is what the actual bad stuff that's happening.

So by leveraging AI you sift through that noise, bubbles up things for them to actually dive deep into what's really there.

Chairman GREEN. The essential is the AI is now fighting the AI, basically, right? I mean, the machines are fighting the machines. Am I getting this right? It is to put it in simplest terms?

Mr. SIKORSKI. I think to some extent. I think there is definitely that kind of thing going on for sure.

Chairman GREEN. Yes.

Mr. SIKORSKI. But at the end of the day the cyber analyst is being up-leveled in their ability to fight back.

Chairman GREEN. Yes. We have got to figure it out. We have got some legislation coming out pretty soon on work force development and I want to just make sure that the AI piece is captured in that.

So thank you. My time has expired.

I now recognize the Ranking Member for his 5 minutes of questioning.

Mr. THOMPSON. Thank you, Mr. Chairman.

You know, one of the things that we have become accustomed to is if we are filling out something on-line as we complete it they want to figure out if you are robot or if you are a human. So you got to figure out. Now, is this a bus or is this a car or is this a light?

So all of us are kind-of trying to figure this out. So you gentlemen have given us some comfort that there are some things out here but let me just give you a hypothetical question.

As we look at this how do you see the role of Government as AI develops and what do we need to do to ensure the public that that development does not allow our adversaries to become even more our enemy than what it is?

We will start with Mr. Demmer.

Mr. DEMMER. Thank you, Mr. Ranking Member, for the question. I agree the country needs to prioritize building AI that is safe with the Executive Order. That, you know, where I stand is that we need to collect highly-accurate data that ultimately informs these models.

Increasingly what I think can be done is to help create test beds for helping to validate those models and creating the training data sets that enable, you know, good AI to be created leveraging only good data sets. So that's my position.

Mr. SIKORSKI. Yes. I think one thing that I think of is my history in cybersecurity. We rushed as innovators to get the internet out and we didn't build that while thinking about security, and look at the spot we're in.

I think that's why it's really important that we build AI and have it secure-by-design. It's one of these things where it falls into a few different categories, making sure that the AI that we're building. Everybody's rushing to get this technology into their products and out to consumers, but we need to think about it as we build it. For example, what is the application development life cycle? What is the supply chain of that being built and is that secure?

Thinking about these things as they're running in real time, how are we protecting those applications so that they don't get manipulated? How about the models we're building? How about the data? Is that, you know, subject to manipulation? How are we protecting that?

Then how do we monitor it? How do we monitor our employees that are all probably using this today without even our knowledge? So those are all areas where I would focus.

Mr. AMLANI. In addition, when building the internet, identity was actually not a layer that wasn't originally thought about. So the challenge that you just described about the changes of buses, I just encountered sea planes versus normal planes, and it's very difficult to try to decipher between what's a sea plane and a normal plane in terms of a captcha. That's the field it's called.

Standards and testing is a very important component here. I think we need to continue and constantly test all the tools to make sure that they're inclusive and making sure that they're accurate. Standards are another important component here that comes out of testing, but it is also very focused on leveraging and organizations like NIST and to continue to invest in organizations like NIST.

Talent development is the other component that I would heavily focus on and much of that resides in the private sector and partnerships with private-sector companies.

At Defense Innovation Unit we surveyed the top 25 engineering schools about where they wanted to work after they graduated, and there was no Government agency other than NASA on that whole list. There was no Defense or a Government contractor on that whole list other than SpaceX.

So as we start to think about this, how do we actually get access to the top engineers across society? That is actually through partnerships with the commercial world. Thank you.

Mr. LAPERRUQUE. Yes. I would echo several of what's been said already. We need well-trained systems. We need high standards for procurement to make sure that we're using good systems. We need proper data inputs to be going into AI systems and proper treatment of what's coming out with human review.

I would also emphasize, though, that beating our adversaries in this field means that we do not end up imitating our adversaries. Right now facial recognition is an example I've already harped on that is used in a frightening way in regimes like China, Russia, Iran. Right now Federally we do not have any regulations on law enforcement use of facial recognition. Although the cases are limited, there are documented cases of it being used against peaceful protesters in the United States. That's a type of standard that we should be prohibiting.

Mr. THOMPSON. Thank you very much.

Mr. Chairman, maybe I will submit for the record.

We have elections coming up in November. The last time there was some involvement by Russia, China specifically with our elections.

Are you in a position to say whether or not we are robust enough to defend against our adversaries for elections? Or are you to encourage us to be a little more attentive to any aspect of our elections?

Mr. SIKORSKI. Well, that's a great question. I think that certainly generative AI makes it easier for malicious actors to actually come after us in that way. We've actually already seen them in the cyber arena start to build more efficient phishing emails, so things like typos, grammar mistakes, all of that kind of stuff, that's a thing of the past. That won't be something we encounter anymore, and——

Mr. THOMPSON. In other words, there won't be any more typos?

Mr. SIKORSKI. Right, and they could also read someone's inbox and then talk like that individual, right?

Mr. THOMPSON. Right.

Mr. SIKORSKI. They could leverage it in that way. I do think that CISA, and we're a member of the JCDC and they're taking, you know, election security is a big priority for them. So, you know, we're assisting in those ways and, you know, I think that it's definitely super concerning and something we need to lean into with the election cycle coming up.

Mr. THOMPSON. Anyone else want to address that?

Chairman GREEN. It is a good question. I will let the gentleman's time continue if anybody else wants to answer.

Mr. AMLANI. I think from an identity perspective this also is very important with regards to who is it that's actually posting on-line and being able to discuss.

So from an identity perspective making sure that it's the right person, it's a real person that's actually posting and communicating, and making sure that that person is, in fact, right there at that time is a very important component to make sure that we know who it is that's actually generating content on-line. There is no identity layer to the internet currently today.

We have a lot of work that's being done on digital credentials here in the United States. Our country is one of the only in the Western world that doesn't have a digital identity strategy. We had some work that's actually been done in the national cybersecurity strategy, Section 4.5, but it hasn't really been expanded upon. I think that's some work that we should think about encountering and doing.

Chairman GREEN. Yes, if I may? You know, I have some questions on that, too, that I might submit in writing because this digital identification thing is, you know, as banking and all of that goes into the wallet and on the phone it is this digital ID is a critical issue. So I will send some questions, too.

Are you good?

Mr. THOMPSON. Yes, I am good.

Chairman GREEN. Thank you, Ranking Member.

I now recognize Mr. Higgins, the gentleman from Louisiana, for his 5 minutes of questioning.

Mr. HIGGINS. Thank you, Mr. Chairman. Mr. Chairman, I have worked extensively with my colleagues on the House Oversight Committee regarding artificial intelligence and I am not necessarily opposed to the emerging technology. Even if I were it would be like opposing the incoming tide of the ocean. It is happening.

I think it is important that Congress provides a framework so that AI cannot be leveraged in any manner that is contrary to Americans' individual liberties, rights, and freedoms.

I introduced the Transparent Automated Governance Act, the TAG Act, as a first step to set limits on Government application of artificial intelligence. As a whole, the bill seeks to ensure Federal agencies notify individuals when they are interacting with or subject to decisions made using a AI or other automated systems and directs Federal agencies to establish a human review appeal process to ensure that human beings have supervision of AI-generated decisions that that could impact the lives of Americans and specifically our freedoms.

So I have concerns about this tech, but we may as well embrace it, because I think it is crucial that America lead in the emergence of AI technologies and how it interfaces with our with our daily lives.

May I say, we could have hours and hours of discussion about this, but I have 5 minutes, so I am going to ask you gentlemen regarding the use of AI as it could contribute toward more effective counterintelligence or criminal investigations as those criminal investigations and counterintelligence efforts relate to homeland security. I am trying to focus in on this committee, our committee here, and our responsibilities.

What are your thoughts, gentlemen, on how we can best deploy AI with our existing law enforcement endeavors for border security and criminal investigations that result from our effort to secure and re-secure our border?

Mr. Sikorski, I would like to start with you.

Mr. SIKORSKI. Yes, that's a great question. I think one thing I look toward is the way we're already leveraging AI for cyber defenses, as I spoke about in my statement. We've been taking really large amounts of data and distilling it into very few actionable items that a human can——

Mr. HIGGINS. You say taking large amounts of data. Where you getting that data from?

Mr. SIKORSKI. So for us as a cybersecurity company we are focused on processing security data, which means ones and zeros, the malware that is found on the systems, the vulnerability enumeration of those systems, low-level operating system information that enables us to, like, tease out what's the actual threat, which is very distinct from——

Mr. HIGGINS. So you are drawing your raw data from open sources and from—like, how are you accessing the raw data that you are analyzing?

Mr. SIKORSKI. Yes. So that's a great question. So some of the data that we're getting is from, you know, the customer collection that we have in our products that are spread throughout the world. It's a total of 93 is the level of information——

Mr. HIGGINS. From the Fortune 100 you said? Your company works with 95 of the top 100?

Mr. SIKORSKI. That's right.

Mr. HIGGINS. OK. So those companies have agreements with their users. That is that part that we don't read as it comes up on your phone and you renew the agreement and nobody reads it. We go to the bottom and click yes.

So in the 95 companies there are agreements to share that data. You are using that to analyze through AI for the purposes of what?

Mr. SIKORSKI. Yes, in order to find new attacks. So one of the things we're doing is it's firewall data, network-level telemetry, host system-level telemetry. It is very different than, you know, say, personal information or something like that.

Instead we're focused on that lower-level data, bringing that together and then leveraging AI to say how is that network attack related to what's happening on the actual computer, bringing that together quickly so that the analyst can find the threat and eliminate it very quickly.

Mr. HIGGINS. You are specifically referring to cybersecurity, but—Mr. Chairman, my time has expired. I have many questions I am going to submit to these gentlemen in writing. Thank you for convening this hearing. It is very important.

Chairman GREEN. Absolutely, thank you.

I now recognize Mr. Carter, the gentleman from Louisiana——

Mr. CARTER. Thank you, Mr. Chairman.

Chairman GREEN [continuing]. For 5 minutes.

Mr. CARTER. Thank you to the witnesses for joining us today. Advancements in AI technology as it demands for its use, possesses significant challenges. We must mitigate the associated risk and threats by leveraging AI to improve our national security.

I urge my colleagues to support my bill H.R. 8348, the CISA Securing AI Task Force Act, which proposes the creation of a dedicated task force within CISA. This task force will focus on addressing safety, security, and accountability challenges posed by AI. Today's discussion is crucial for the American people as we work to tackle these pressing issues.

AI is not new. We know that. It is relatively new to the general public and some of its applications have enormous value. Some of them can be quite frightening.

National security, obviously, is major so I would like to ask each of you to take a crack at answering the questions relative to civil rights, civil liberties, and privacies in general for the American people. How is this contemplated as we develop further delving into AI?

Mr. Demmer.

Mr. DEMMER. Well, I'd defer to my fellow witnesses on this issue given their expertise, but it is certainly worth a spirited conversation about how we balance national security and civil liberties. What I can say is Gecko is focused on building the datasets on most critical infrastructure in a way that promotes national security.

Mr. SIKORSKI. So I'm a cybersecurity practitioner, as I said, so I'm not—you know, don't know all the ins and outs of the policy itself, but my sense is that when we think about AI and regulation we've got to think of the purpose. So defining what is high-risk, right, and then saying, you know, what are the AI use cases that are actually high-risk, and focusing on the unique security requirements for them.

On the cybersecurity side I think that security data, those ones and zeros I was talking about earlier, are a little bit not high-risk compared to a lot of other technologies that are being rolled out.

Mr. AMLANI. At iProov we take inclusivity by design very seriously. We do regular self-assessments on our own technology. We work with every single independent assessment organization that's out there.

We're encouraging more independent assessment organizations. We're encouraging them to stay ahead of the technology. Many times these independent organizations focus on threats or challenges in the past. We need to stay up to speed. We need to stay above and go beyond.

We build inclusivity by design, as I mentioned. That includes, obviously, skin tone but also cognitive and physical capabilities, making sure that those are taken into consideration in inclusivity, socioeconomic class as well.

Many technology tools are expensive to be able to attain. I just got the iPhone 15 Pro and I can attest to that. Age is also a very important component, as well as gender.

So making sure that all of those different characteristics of inclusivity are also embedded into the design of the AI is an extremely important component of success.

Mr. LAPERRUQUE. So there certainly is a range. Some systems like, for example, damage assessment systems that DHS uses present lower risks to maybe no real risks to civil rights and civil liberties. Other technologies such as facial recognition, mobile device analytics, or automated targeting systems, all of which DHS employs, present very significant risks to civil rights and civil liberties.

The OMB memorandum on AI puts a good stress on care for civil rights and civil liberties. We hope that's a good step toward development of strong internal guidelines within agencies, but this is an area where transparency and oversight are essential to evaluating the effectiveness of those rules, evaluating whether more steps are needed, and, as necessary, prompting Congress to step in and make their own rules.

As I mentioned, in the field of facial recognition there's no current Federal laws or regulations for law enforcement use. We think that's something that needs to be changed.

Mr. CARTER. So the information out is only as good as the information in, so the data becomes paramount. So how do we take into account cultural nuances, natural biases so that we are not replicating biases that humans have and then become a part of the bias that is in AI?

Mr. Amlani.

Mr. AMLANI. At iProov we have a world-wide deployment and so we operate in Singapore, we operate in Australia, in the United Kingdom, in South Africa, in many African countries, as well as Latin American countries as well as North America.

We take very careful consideration that basically making sure that we're seeing all of the threats coming in from all of those locations but also taking into account all of the data and making sure that we have a representative database that we train on.

We go over and above when it comes to making sure that our training data is, in fact, representative of the overall population. I would encourage you to be able to include standards and testing and invest in those to make sure that other providers are also doing the same.

Mr. CARTER. So from our standpoint, obviously, as you have heard from the questions here, you continue to hear that Congress has real concern on making sure that we learn from the—mistakes may not be the right word but we learn from how fast the internet came, Facebook, Instagram, and all of those things. They are constantly bringing about new challenges, the good, the bad, and the ugly.

How do we learn from that to make sure that we are managing this AI as it unfolds and becomes more prevalent in our society?

I realize that my time has expired, so, Mr. Chairman, if you would allow them to answer, that I will yield.

Mr. HIGGINS [presiding]. The gentleman can answer the question.

Mr. AMLANI. Sure. That's directed at me, I assume?

Mr. CARTER. Yes or anyone else who cares take a crack at it.

Mr. AMLANI. Thank you, Congressman. Staying on top of all of the different technologies is very important in making sure that we have independent organizations within the Federal Government that can have different companies submit their AI to testing and making sure that we have the right people staffed within those organizations who can stay on top of all of the latest opportunities and threats in the market.

Yes, there is a lot of interest that this overall industry has in making sure that basically its well-represented databases and common standards that we can all adhere to. I think making sure that those accurate solutions can be in front of the customers for biometric verification is also a very important component.

Biometric verification it is also something that's very different than biometric recognition, and I want to make sure that we can call out the two differences between the two.

Mr. HIGGINS. The gentleman's time has expired.

The Chair has been flexible and generous with time, but I ask all Members to watch the clock.

The gentleman from Mississippi, Mr. Guest, is recognized for 5 minutes for questioning.

Mr. GUEST. Thank you, Mr. Chairman.

I want to thank all of our guests for joining us today. As we have we seen the incredible growth of AI, we know that AI can be used to gather and analyze data. We know that AI has both offensive and defensive capabilities. With all technology that AI can be used for good and evil.

But specifically as we drill down today on homeland security and looking at the role that AI is playing in homeland security, I think it is easy for many of us to see the role that AI plays in cybersecurity. We have heard testimony about the offensive and defensive capabilities of AI in the cyber world, but I want to talk a little bit about the role that AI may play in securing our physical borders.

One of the things that this committee has been focused on is trying to secure our Southwest Border. We know that last year there were 3.2 million encounters on the Southwest Border, a record number of encounters, that we are on track to break that record again this year.

We know from statements that the Secretary of Homeland Security has been reported that he has made that 85 percent of those individuals encountered are at some point are released into the interior. So my question is how can we use AI to better identify the individuals that are being encountered? Because I have a great fear that we are not identifying and properly vetting those individuals before they are released into the interior.

I will start with you, Mr. Amlani. You talk a little bit in your written testimony about biometrics and the use of biometrics and the Maryland biometrics test and their facility and the things that you all are doing.

So I would ask maybe first if you could start off and then if anyone else would like to join in, how can we within the Department of Homeland Security better use AI to identify the numerous individuals that we are encountering on a daily basis along the Southwest Border so that we are not allowing people into the country that would cause ill will, people who may have criminal records, criminal backgrounds?

We see people all the time who are apprehended that they may have a tie to some sort of a terrorist organization or individuals who have previously been arrested and convicted of violent crimes in other countries. So how can we use AI to better vet those individuals, to do so in a more timely fashion before they are released?

So I will start with you, allow you to kick that off, and then would ask anyone else who would like to join in to please continue in this discussion.

Mr. AMLANI. Thank you, Congressman, for the question. This is a very important question in my mind. We at iProov, obviously, cannot speak on behalf of DHS, but I can speak upon behalf of my experience in 2003 at the Department of Homeland Security originally launching new technologies like biometrics at the border.

Secretary Tom Ridge did assess biometrics as one of the core technologies to be able to improve the Department's capabilities, improving throughput as well as being able to improve security at the same time.

My personal experience with biometrics was actually introduced to me first in 2003 US–VISIT program when it was rolled out at airports for the first time for people coming into the country that were not citizens. We actually used fingerprint technology at the borders.

It was very eye-opening for me for people walking up to a Customs and Border Patrol agent who had a look of fear in their eyes, about to be asked a significant set of intrusive questions and disclosing a lot of private information, who then put their fingerprint down on the device and to have the Customs and Border Patrol agent say welcome to the United States.

That sole interaction for me was something that lit a fire within me over the last 20 years to recognize that this was not just a security tool and a capability that was focused on law enforcement, but actually a tool for consumers to be able to allow themselves to be able to protect their own privacy and have better experiences.

Mr. GUEST. Anyone else like to add in?

Mr. LAPERRUQUE. Yes, sir. I would just add that this is, I think, a very good example of how input data, what you're putting into a system, and the quality can make such a difference.

In biometrics and facial recognition fields a photo that is done, good lighting, close up, clean profile such as a DMV photo or a photo during processing and booking, that is much more likely to yield accurate results than, say, for taking something in the field from a distance, if I just took my smartphone and tried to click a picture of you now, or if someone was taking a photo at night.

So it's, I think, a prime example of when you're talking about something like during processing why those different situations can make such a difference about whether AI is reliable or not. It really is highly situational.

Mr. GUEST. Would either of our other two witnesses? I will give both of you an opportunity before I yield back if anyone would like to add to the discussion?

Mr. Chairman, I am over time so I yield back.

Mr. HIGGINS. The gentleman yields.

The gentleman from Maryland, Mr. Ivey, is recognized for 5 minutes for questioning.

Mr. IVEY. Thank you, Mr. Chairman, I appreciate that.

To my Republican colleagues, if you will relay to Chairman Green my appreciation for having this hearing, I think this is an outstanding topic for us. In fact, we might even need to have additional hearings on this topic because the time goes so quickly, but thanks again for having it.

To Mr. Amlani, welcome from Maryland. I represent Prince George's County. You are just outside of our district. Hopefully when that lease comes up we can convince you to move a little further south, but we will take it one step at a time.

I did want to ask the Whac-A-Mole question to you, Mr. Sikorski, because that is something I have been kind-of worrying about quite a bit. We have identified a lot of threats and the challenge, I think, is that sometimes they can replicate very quickly, faster than certainly a litigation approach can remedy those.

Let's take the, you know, deep fake types of imagery. We have had some of those pop up. Sometimes they are aimed at embarrassing individuals, sometimes, you know, revenge porn kind of things.

So since I don't know that litigation is fast enough to do it, and I think you mentioned that your company has taking some steps to try and deal with that moving forward, I'd like to hear a little bit more about it.

But in addition to that, how can the Government create incentives for the private sector to do more on that front? Because I think it might have been the Ranking Member mentioned, you know, you've got AI fighting AI? I think that is going to be better than Government fighting AI or certainly the courts.

How can we go about it in a way that allows us to keep pace?

Mr. SIKORSKI. Yes. That's a great question, Congressman. I think there's some things that are already happening that are really great with the Government, a few things that I'm actually pretty passionate about myself, things like collaborative defense.

So back when I worked for the NSA you didn't tell anybody you worked there. Now, there's a cyber collaboration center that reaches out to industry and realizes that we can go much further with defending the Nation if we work together versus in complete and utter silos.

So continued push, like we've seen with CISA and the JCDC, for example, has been very successful and is moving the needle. So keeping pushing hard on that front, I think, is imperative.

I also think that it's important to think about cyber hygiene and what entities are doing. So companies that are out there, how are they protecting themselves?

I think CISA offers a great range of cyber hygiene and vulnerability scanning services, for example, which is great, but one thing we lack somewhat is, like, what's the report card on how efficient somebody's cybersecurity is, especially when you talk about critical infrastructure, health care, and so forth.

So maybe we should roll out metrics that we could actually track over time like Mean Time to Detect, Mean Time to Respond, how quickly are we actually responding to attacks and sifting through all that noise?

Mr. IVEY. All right. I want my monitor my time, but just to follow up, if you could respond in writing perhaps, but the Unit 42 Academy was very interesting to me. I was wondering how that might be replicated?

Perhaps are there ways that the Government could encourage other private entities or, you know, colleges and universities that might be willing to do it? But find ways to expand that effort, too. The too-many-alerts points that you made earlier is another one I would like to find out a little bit more about.

With respect to talent development, I appreciate the fact that, you know, there are efforts going on and, Mr. Sikorski, I think your company mentioned that and, Mr. Amlani, I think you did as well. I think that is going to be a good solution for the intermediate and long term.

In the short run, you know, I think we are importing a lot of the talent, and in some instances we have had people come and testify before this committee that they are coming from hostile states, frankly.

So one of the things that I am wondering about since the Government monitors it to some extent on the way in through the, you know, the immigration process which has its challenges for sure, even with respect to these types, but the other is once these guys get in and they go to these companies how do we know that the company is doing a good job of monitoring these individuals to make sure that they are staying on the right track? They are not misusing their position? There is no economic espionage going on?

Should we be confident that these companies are doing a good enough job to make sure that the United States is protected and their industries are protected from those sorts of potential attacks?

I apologize to the Chair for running over the line——

Chairman GREEN [presiding]. Please.

Mr. IVEY [continuing]. But I appreciate the Chair's indulgence on this.

Anyone who would like to answer?

Mr. SIKORSKI. Yes, that's a great question. I think, you know, I've been doing incident response for almost 20 years and it varies. It's not just nation-states that have threats. It's not just ransomware.

Another big threat is insider, and we see insider threats when Unit 42 is responding where, you know, it's not just the threat of them maybe putting something into the supply chain and getting it out the door and that kind of threat, which we know nation-states are embedding employees in that way, but also we've seen where they go out the door and then they have stolen data.

Then they start engaging in ransomware-like behavior, especially if their country doesn't have the ability to make money and has their economy cut off. So those are just some ideas I had.

Mr. IVEY. Anyone else?

Well, Mr. Chairman, thank you, and I yield back.

Chairman GREEN. Yes, of course, and I appreciate it. I did see your kind words when I was out in the lobby section out there, so I appreciate that.

I will tell you that I think, honestly, and I would ask Members for feedback on this, we need more, you know, the 5 minutes in a hearing room just aren't getting it, right?

So what I may do is have, like, a town hall-type thing where we are the town hall and they are on there and we are just asking questions. It is more. I think that would be more informative and maybe some presentations, so to speak, on data poisoning for AI and all that kind of stuff and then us understanding a little better to ask more informed questions.

So thank you for saying that. Work with me and we will get some more stuff on the books for this.

Mr. IVEY. I appreciate that, Mr. Chair.

Chairman GREEN. I now recognize Mr. Ezell, the gentleman from Mississippi, for his 5 minutes.

Mr. EZELL. Thank you, Mr. Chairman.

Thank you all for being here today and helping us out here. This is something that we all are concerned about, and we appreciate you being here today.

The capabilities of AI are quickly advancing. This product which when I look at it feels futuristic, holds the power to significantly improve the way we work and go about our daily lives. However, we also know that advancements in technology create new opportunities for bad actors to operate effectively.

Our great Congress must be closely monitoring this powerful tool to ensure the application is not misused, but the Government cannot get in the way of American leaders in this sector and their ability to improve the product. The Chinese Communist Party has intense ambitions to win the AI race.

As I talk with people in the private sector, it is clear we are in a global AI arms race. Our adversaries are innovating quickly and it is critical that we do not restrict the capabilities of American business.

I would like to just direct this to the entire panel. How can we ensure America's leadership in AI and what Government actions could jeopardize this? Start with anybody who wants to answer.

Mr. AMLANI. Thank you so much for the question. This is a really critically important point for me. I think continuing to stay ahead of our adversaries on technology requires both investment in our talent and work force.

I just took my 15-year-old son on college visits and I can tell you it's actually very difficult to be able to get into an engineering university today.

I think that there's an unprecedented demand for people wanting to study AI and wanting to study cybersecurity and wanting to study other types of engineering that are being left out of the work force that are there at the college stage. They get intimidated by software engineering.

Being able to make that a part of the high school curriculum leading into college I think will also help and then creating more educational opportunities for individuals wanting to be able to get into the work force and learn those skills, not just at the college age, but also going forward as they are progressing through their careers.

In particular, investing in companies and making sure that we are actually hiring companies that have the best talent is another component. Those companies themselves can recruit the best talent. They provide entrepreneurial worlds that allow individuals to be able to create and solve problems in settings that are fun environments to be able to do that.

I think if we can actually make a concerted effort through organizations like the Silicon Valley Innovation Program to hire the right companies to be able to solve some of our massive Government problems is an important component to stay ahead.

Mr. EZELL. Thank you very much.

Anybody else like to say anything?

Mr. LAPERRUQUE. I would say that encouraging, whether it's by a procurement, other incentives, responsible development of tools and proper use of those tools is key in making sure that we're not simply trying to barrel ahead with reckless development or reckless applications. That's not going to yield good results.

As I said before, winning the AI arms race doesn't just mean the fastest and broadest build-up. It means the most efficient and effective one.

It's also, I think, a matter of looking at our values. When we look at countries like China, Russia, et cetera, it is a deployment of AI that is draconian in nature and that has supported those authoritarian regimes. So I think it's important that we be not just a global leader in innovation but a global leader in values in this space and making sure that when we're promoting the use of AI we're promoting a use that is in conjunction with democratic values.

Mr. EZELL. Thank you very much.

Mr. Sikorski, China limits its citizens' access to information through censorship, and I assume they will continue these restrictions on AI. How does America's freedom and the capitalist economy help to attract global investment around AI?

Mr. SIKORSKI. Yes, I think that's a great question, and I think that one way that we do is just by that fact we're a little bit more open with regards to how we're able to innovate and in what regard we're able to innovate.

I think as, sort-of, putting that together with your previous question, I think about, you know, what is the high-risk AI models we're building that are impactful to our citizens? Things like maybe somebody applying for credit or for university, right? Those kinds of things are high-risk and maybe something we should need to hunker down on as far as, you know, how are they being built up? Versus on the cybersecurity side, I think the risk is a lot different and, therefore, like, really pouring in a ton of innovation, which we're doing in industry and we see organizations like CISA doing. So us coming together with the Government to really iterate fast and thinking about the charge of how do we sift through the noise, which I've talked about a few times of all this security alerts and actually make sense of it to find, you know, the next big attack.

Mr. EZELL. Thank you.

Mr. Chairman, I yield back. Thank you all again.

Chairman GREEN. The gentleman yields.

Now, as Chairman I will take a privilege here just a second and shamelessly plug the academic institutions in Tennessee, the Vanderbilt University just hired General Nakasone to become lead cyber and the University of Memphis, University of Tennessee are doing some exceptional research with Oak Ridge and Redstone.

Of course, Tennessee Tech, one of our engineering programs, your son should check that one out, too, an outstanding one. They go out to high schools and middle schools and they are starting cyber to very early age. Great, great schools in Tennessee. Sorry I just had to do that, guys.

I now recognize Mr. Magaziner for 5 minutes of questioning. He snuck in on you. Oh, I am sorry, but he——

Mr. THANEDAR. Yes, it is——

Chairman GREEN. Mr. Thanedar, I am sorry. I looked at the nameplate. You are——

Mr. THANEDAR. Well, my name is Shri Thanedar. I represent Michigan and Detroit, and my question is for Mr. Sikorski. You mentioned in your testimony the need to secure every step of AI app development life cycle.

As we saw with the Solar Winds hack, a supply chain vulnerability can have far-reaching consequences. Can you speak in more details about what steps Palo Alto Networks takes to minimize supply chain vulnerabilities?

Mr. SIKORSKI. Yes, that's a great question. Actually I was heavily involved and actually led the team that reverse-engineered the Solar Winds back door, which was pretty exciting to get to brief Homeland Security about that as we were unboxing it.

I think about, you know, that is one of the biggest concerns we have when we think about cyber threats is the supply chain attack. We've seen there's been numerous other examples since Solar Winds which is now a few years in the past, where our adversaries are able to get into that supply chain, deploy code, and then it gets shipped out to customers which then essentially gives them a back door into networks.

At Palo Alto Networks we're really focused on thinking about how to eliminate that as you're building your code and as you're shipping out your products. So as I mentioned, there's sort-of multi-different tiers that we're thinking about when it comes to AI security, but one of the biggest is absolutely the supply chain because people are very quickly developing this.

They're pulling in technologies that are out there on the internet or otherwise and that makes a really good opportunity for an adversary to slip something in. So we adopt technologies and are really focused our AI on eliminating those threats.

Mr. THANEDAR. Thank you. Can you elaborate on what shortfalls the AI industry has demonstrated when it comes to securing AI app development life cycles?

Mr. SIKORSKI. I'm sorry, what was that? The horn is——

Mr. THANEDAR. Can you elaborate on what shortfalls the AI industry has demonstrated when it comes to securing AI app development life cycles?

Mr. SIKORSKI. Yes. I think one of the things I think of is, you know, when we're rushing out new technologies we're often not taking the time because, you know, often what happens is there's companies that are pitted against each other and who can get this AI technology out to their customers first will win the industry. Like, that's what we're talking about is to how fast AI development is working and we've all talked about how much it's going to evolve our life over time and it's inevitable.

I think that when you do that people end up rushing, doing things, and cutting corners to get those technologies out, not thinking about security. Shocker. That's the thing we dealt with a lot of innovation over time.

I think that making sure that we're actually putting in mechanisms to think through how what is people's security posture? Are they doing the right things as they're shipping out applications because to a large extent software development in our country is a national security issue when we talk about the supply chain.

Mr. THANEDAR. This is a question for the whole panel. The world has not yet seen a major AI-driven cyber attack. On the scale of attacks like NotPetya or WannaCry, what is the likelihood that we see an attack on this scale or worse in the next 5 years? Anybody.

Mr. SIKORSKI. I'll take that one as well, you know, as a cybersecurity guy. So one thing I think about is that is an absolute threat and huge concern I have because we saw ransomware spread like wildfire, take down systems with NotPetya, like you mentioned. The shipping industry was impacted with that and I remember seeing, you know, grocery stores for one of the big chains just completely knocked out. People couldn't even buy groceries.

Then I also think about my experience with Solar Winds and the fact that just imagine that Russia was using AI in that attack. They would have been able to focus more on getting their hooks into systems for which the Solar Winds attack gave them access.

If they could have done that in an automated way rather than using their human army, it would have been much more of an efficient attack.

Mr. THANEDAR. All right. Anybody else?

Mr. LAPERRUQUE. Thank you. Yes, I'll just—it's a serious challenge because it's a type of scenario where AI can be the weapon or it could be the target. So as we've discussed a bit here, it might be something that's used to facilitate a phishing attempt. You could use something like a deep fake to augment a phishing attempt maybe instead of just sending an email and then you get a fake call, voice message, or even a video saying, oh, open up that email I just sent you. That makes someone less suspicious and helps facilitate that.

It's also potentially a target point. Critical infrastructure they use lots of AI systems in ways that might not at all be related to national security, but if there's a vulnerability there or there's some sort of manipulation of AI systems then that could also be a vulnerability point maybe.

Perhaps, you know, how we might use AI to distribute power along the grid or how we use it to check to people coming into a stadium or a large-scale event. If those AI systems and the algorithms behind them were a target of an attack or subject to manipulation that could raise a host of risks.

Mr. THANEDAR. Thank you so much.

Mr. Chair, I will take my own seat next time. Sorry for the confusion.

Chairman GREEN. So you don't confuse me, yes. I got it. Poisoned the data there. Thank you and sorry I got your name wrong.

I now recognize the gentleman from Texas, Mr. Pfluger, for 5 minutes of questions.

Mr. PFLUGER. Thank you, Mr. Chairman. I think it is an important discussion. I am glad we are having it.

Thanks to the witnesses for being here.

The public-private partnership that we have throughout the United States between Government, you know, including Department of Homeland Security and other agencies, and then private industry, including and I think importantly critical infrastructure, I don't know that it has ever been as important as it is today.

So I think the witnesses for being here because I think the goal is for us to be able to keep up. One of the ways that we can keep up and one of the ways that we can continue to train the next generation is actually happening in my hometown at Angelo State University.

They are a cyber center of excellence. They are a Hispanic-serving institution. I think that is very important. It is a very rural area, but they also have a very strong focus in addition to just general cyber issues on AI.

In San Angelo we have Goodfellow Air Force Base, which is a joint intelligence training base. So you pair these up together you have got university work being done. You have the military that trains our intel professionals, a majority of them train at that location. So I want to put a plug in there for that and I may ask some questions on that.

But let me go to Mr. Sikorski. In your testimony you talk about how adversaries are leveraging AI, and I would just kind-of like to get whether it is phishing or some other older technique or whether it is a new technique maybe talk to me about how you see adversaries increasing the scope, the scale, and actually the threat using AI?

Mr. SIKORSKI. Yes. That's a great question, Congressman. I think that, you know, it goes to the question earlier, right, like, the what if some of the attacks we've seen in the past leveraged AI in a large-scale attack.

I also think about the evolution, right? So the first thing that the attackers want, and we're monitoring them, you know, one of the things Unit 42 does is threat intelligence so we're monitoring the dark web. We're seeing what they're talking about in their forums, what they're selling to each other, their access to networks, but also talking about how to leverage this technology to create really efficient attacks.

The big focus so far has been on social engineering attacks, which means things like phishing, which we talked about, to get you to click on something you wouldn't otherwise. Then also manipulate you to get, like, multifactor authentication, you know, where you need that extra token to log in? They're really focusing there as well.

Where we start to see them, you know, poking around is using AI to be able to do better reconnaissance on the networks they're attacking to know, you know, what holes are in networks across the world.

Then also they're starting to wade into how can they develop malware efficiently and variations of it so that it's not the same attack you see over and over again, which goes back to the point of how do you fight against that, which is you need to develop technologies that are really efficient using AI to see those variations.

Mr. PFLUGER. I want to ask all of you in the last 2 minutes to speak to this model that Angelo State University is using where they're training students. Those students may go into the NSA. They may go into the military. They may go, you know, in the private sector. What should Angelo State and other universities be doing?

We will start with Mr. Laperruque and then go down. We have about a minute and a half.

Mr. LAPERRUQUE. I mean, I'm not a hard science person so I probably have less to add than my colleagues, but I would just say I think I have found in my field it's invaluable for people in the policy space like me to learn from the people who understand the tech, and people who are developing the tech to understand and to learn from people who are experienced in policy, experienced in protecting civil rights, civil liberties, and values.

You know, it helps with sort-of how we can translate across to each other and also helps as you're designing these systems to think about what's the best way to do it and how we can actually do it in a way that's going to promote what we care about as a society.

Mr. PFLUGER. Thank you.

Mr. Amlani.

Mr. AMLANI. I think, first of all, I think actually there's a vocabulary around cybersecurity that is a very important component to be able to educate our youth on everything from spear-phishing, you know, you mentioned all the other types of attacks. I think these are important things to be able to teach people about to make sure that they themselves are not hacked, but also they understand what the attacks are actually happening and how to guard against them.

Identity is a big, big component of all cyber attacks. It's about 91 percent of all cyber attacks are actually originated with a credential that's been stolen, that's been hacked, that's been compromised in some way, shape, or form.

Then malware gets implanted within a system that can then be activated afterwards on an on-going basis. So having better identification mechanisms to make sure that individuals don't have to change their password every day, they don't have to have multiple things that are very hard to remember——

Mr. PFLUGER. Would you say that the universities should be researching this? That they should be doing it in maybe even a Classified setting that they should be working on these types of techniques and partnering with Government agencies as well?

Mr. AMLANI. Government agencies as well as commercial sector as well.

Mr. PFLUGER. Very good.

My time has expired. I am sorry, Mr. Demmer. I didn't get a chance to talk to you, but I yield back.

Chairman GREEN. The gentleman yields.

Mr. Suozzi, I think Mr. Menendez has asked that you go ahead of him and so you are recognized for 5 minutes.

Mr. SUOZZI. Thank you, Mr. Chairman. Thank you so much for doing this hearing. I am very interested in the idea of you doing some, sort-of, offsite retreat where we could delve into this in more depth.

Thank you to the witnesses. When I listen to you and I think more and more about AI the more terrified I become, quite frankly. I know there is great opportunities but I am scared.

In 1974, I was in seventh grade and I remember Sister Ruth at St. Patrick's grade school saying, you know, technology is moving so fast these days that we don't have a chance to figure out how it is affecting us, how it is affecting our values, how it is affecting our families, how it is affecting our society, how to effectively—it is just moving too fast.

That was, you know, because of the space race and electronics. You know, Atari had just come out with Pong in 1972 or something, so, you know, think about how fast everything is moving now.

You know, think of all the impacts we have seen from social media on our young people where these polls come out and say, you know, 35 percent of kids are patriotic whereas, you know, for Boomers like me it is 70-something percent. Nobody believes in any religion anymore or any institutions and we have all these kids with mental health issues related to their self-esteem.

So everything is moving so quickly and I am confident that you are going to figure out how to protect, as Mr. Sikorski talked about. He represents 90 of the Fortune 500, and we are going to fight our way through to protect our businesses to make sure that they are looking out for their security and interests.

Hopefully we will think of more things with our Government, but I am worried about our kids. I am worried about our senior citizens getting scammed. I am worried about people using our voices to say things we didn't say.

I am worried about our society that is so divided and our foreign adversaries, the Chinese Communist Party, Russia, Iran are trying to divide us more by using social media and our freedom and certainly using, I think, AI and deep fakes to try and divide us even more.

So I am worried about this divisiveness. I am worried about fraud. So I am going to give you the rest of my time and I am asking each one of you.

You just talked about values, Mr. Laperruque. I am worried about the values in our country, just like people that believe in our values. Forget about the fact that there are other countries that don't believe in our values at all. I am worried about our own country and our values and promoting those values.

So each of you just give me 30 seconds each, if you can. What is the No. 1 thing on the big picture you think we need to be focused on right now to address not the positive parts of AI but the scary parts of AI? So what is No. 1 on your mind?

Mr. Laperruque, you go first.

Mr. LAPERRUQUE. I would say it has to be a comprehensive approach from the creation of systems to input of data and inputting in proper situations to retrieval and use of results. That's something that there ought to be a lot of factors to bring together in the national security space because it's so often veiled in secrecy. That means we have to find mechanisms for transparency and oversight because you don't typically have that sort of light that you can shine on potentially in the private sector and business practices or even other parts of government. So I think we have to find ways to promote that oversight and making sure that we're upholding those principles for responsible use, even when you don't always have the same level of public insights to——

Mr. SUOZZI. So oversight to watch the input of data?

Mr. LAPERRUQUE. Oversight on everything from procurement to what data is being input to how you're using data, what kind of human review and corroboration you have, how much you rely on it. It has to be——

Mr. SUOZZI. That sounds awfully big effort. OK.

Mr. Amlani.

Mr. AMLANI. I mean, as a father of 3 children, all of whom use digital tools regularly, I think first off we're placing a large responsibility on parents to be able to monitor the digital communications of our children.

There aren't the age verification mechanisms currently today to be able to provide a gateway to make sure that the right people are accessing the right systems at any point in time. I think it goes back to the identity layer of the internet that I mentioned before.

As you mentioned, there's all kinds of on-line bullying, you know, extremism, recruiting, other things like that that are happening on-line and it's all being done, you know, not just in the dark web but actually out in the open.

But it's because we don't have the ability to be able to properly recognize who people are on-line and it creates mechanisms and difficulties for making sure that we can actually have stronger values enforced and allow parents to be empowered.

Mr. SUOZZI. OK, better ID'ing people.

Mr. Sikorski.

Mr. SIKORSKI. Yes I agree with both those takes so far, but the other one that I would consider and put out there is the education piece. So I talked heavily already about cyber education and the work force that's going to defend the Nation next as being paramount, but there's also an education piece for the rest of society when it comes to security and AI and being in disinformation, right?

Knowing that what you're seeing on your phone may or may not be real, right? People in an age where people are getting their news by just scrolling through their phone second after second I think that's something that really needs to be considered.

Then how do we eliminate those kinds of things that are not real?

Mr. SUOZZI. Mr. Chairman, can we let Mr. Demmer answer? He hasn't been able to answer a question for a while. Go ahead, Mr. Demmer.

Mr. DEMMER. Thank you for the question, Congressman. You know, I agree with you on the societal and technological advancements, you know, creating some downstream maybe impacts that are unintended.

I personally believe that technology advancement that is happening today, you know, creates a promising future for all workers to be able to upskill, have more fulfillment in their work, and to be enabled with these tools of technologies but it all starts with the critical data.

If we don't have good data going into these systems, then, you know, garbage in, garbage out.

Mr. SUOZZI. OK, thank you.

Thank you, Mr. Chairman.

Chairman GREEN. The gentleman yields.

I now recognize the Chairman of the cyber subcommittee, Mr. Garbarino, for 5 minutes of questioning.

Mr. GARBARINO. Thank you, Mr. Chairman.

Thank you to all the witnesses for being here.

My colleague just before, he was talking about 1974 and Sister Ruth and I was, like, where was I? Oh, wait, I wasn't alive, so 1984, though.

Mr. Demmer, recently one of our biggest concerns has been the prepositioning of Chinese state actors in U.S. critical infrastructure, meaning their posture for a cyber attack if conflict with the United States were to arise.

The U.S. intelligence community has said that AI has been helping them detect this activity given it is much more challenging to decipher than traditional tactics that involve malware injection. How have you been thinking about this challenge?

Mr. DEMMER. Absolutely. So the threats are dual and there's the cyber threats that I think, you know, there's others on this witness stand that can best answer that on the on the physical infrastructure, specifically our critical assets, is a vulnerability. We've seen that.

You know, Gecko's a proven partner for the U.S. industrial base on both public and private sector, and we need to ensure, you know, energy security, you know, critical infrastructure like roadways, bridges, dams. These are all susceptible to physical attacks and, ultimately, you know, creating wins for the industrial base enables us to fight some of these other existential threats as well.

Mr. GARBARINO. Thank you, I appreciate it.

Mr. Sikorski, I understand that you teach cybersecurity at Columbia University, which undoubtedly means that you have a front row seat at our Nation's cyber talent, up and coming cyber talent. In your view, what does the Government need to do to bring sufficient numbers of people into the cyber work force?

Mr. SIKORSKI. Yes it's a great question. I think back to my experience, right, when I was in school it wasn't until I was a senior in college in New York City and 9/11 happened that I was, like, I want to go work for the NSA. Like, that's what I want to go do.

But I didn't really think about that before. It was things like video games and stuff like that, right? I think getting people excited earlier on is a really good place that we can focus, right, of, like, there's cybersecurity hacking clubs, like, at universities and high schools and this gets people really excited to gamify it and play along.

So I think, you know, while we look at the work force gap I think as Palo Alto Networks goes, I already mentioned our work force capability where we have, like, the Unit 42 Academy where we're bringing people in and who don't maybe have the hands-on experience. We're giving it to them with on-the-job-training.

Then I also think about Government programs like I was in when I went to NSA. I was in a technical development program there where I got ramped up on all the things that I didn't learn during my education previous to that. So those types of programs that are feeders, I think, are really powerful in getting people to level up the skills that maybe they didn't get during college.

Mr. GARBARINO. So that was actually, you know, you pretty much already answered my second question. How does it—well, not technically, not all the way. You have these clubs. You have these feeder organizations. What is Congress' role in further improving those or do we have a role?

I mean, how do we—because it is, you know, over half a million jobs, cyber jobs openings in the United States. I mean, that is what keeps me up at night, you know, that we don't have the work force to defend against these cyber attacks.

AI can only bring us so far. We still need that human element, so do we have a role and what is it, if you have thought that far?

Mr. SIKORSKI. Yes. I think absolutely do. I think there's an ability to create these types of programs, right, where it makes it really easy for people to apply and get into, to the point made earlier, about, hey, it's hard to get into schools that have these programs available.

I think we often think that, oh, well, it needs to be a very specific cyber program that they're doing. Some of it is they can learn those types of skills on the job when they get in and it's more about building out the broad base of technical capability in our work force. I think that that's, you know, one great area.

I do think that there's a lot of Government agencies like CISA that have information out there where people can learn and train up. I think there's a lot of virtual education kinds of things going on that are very powerful.

So I think just thinking about how to drag in that work force and some of that is even earlier on, right? So we're talking sometimes giving people skills.

I remember when I taught the FBI it was, like, all of a sudden these people were cyber agents and they had none of the background in cyber. Everybody had no technical computer science background and it was really challenging.

So it's not just a snap your fingers, train them up in a month. It starts earlier.

Mr. GARBARINO. Yes. I think I am out of time but companies, I think, need to start focusing on skills-based hiring instead of degree-based hiring. I think that will help, too.

Chairman, I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the Congressman who represents Palo Alto, I think, yes? Yes. Mr. Swalwell for 5 minutes of questions.

Mr. SWALWELL. Chair, thanks for holding this hearing. It is so important.

Chairman GREEN. Absolutely.

Mr. SWALWELL. I think we are at our best as a committee when we are taking on issues like this. I have enjoyed working with the gentleman from Long Island, Mr. Garbarino, on the cyber committee. I think we are doing a lot of good work there.

Mr. Laperruque, I was hoping to talk to you a little bit about something that Californians are very concerned about and creatives everywhere. You know, the entertainment industry is the second-largest jobs engine in California and it is not just folks who are on screen. It is folks who are writers, editors, part of the production teams off-screen.

AI certainly it is the future. There is no ignoring it. There is no putting it back in the bottle. It is the future and so we have to embrace it. We have to shape it, put guardrails on it, and contours around it.

But when it comes to the creative community, you know, the example over the weekend of what happened to Scarlett Johansson with her voice essentially being stolen from her for an AI product, what should we be thinking about to make sure that we protect artists and creators from this, but still, as I said, embrace AI and recognize that this is where we are going?

Mr. LAPERRUQUE. Well, I think it's going to be important that we find ways to sort-of try to be proactive in anticipating what people's rights are going to need to be. I mean, a situation like that, I mean, you know, probably not something that was even imagined or contemplated when the movie where she played an AI I think it was 4 or 5 years ago came out.

This is something that's come up a lot, I think, in the recent writers' strike, the actors' strike is how do we build in those protections now, not just for how AI is being used right now in this industry, but also how is it going to be used in 5 years? How is it going to be used in 10 years?

So, you know, looking at workers' rights is a little outside of my field, but from just the technology standpoint it moves so fast I think it's important to be proactive in thinking about not just current risks and factors to care about but what do we need to care about down the line that we might not be ready for when it comes up?

Mr. SWALWELL. When you talk to creatives they are not opposed to AI and that is such a basic hot take, which is, oh, they oppose AI. They don't oppose AI. They just want rights and they want—you know, and they are willing to engage around their likeness and their voices, but they should be compensated.

The majority of people who are writers and actors are people you have never heard of, but this is their livelihood. In California we are especially sensitive to that.

I wanted to ask Mr. Amlani because we are in the same backyard in the Bay Area, and the Chairman alluded, you know, that our tech culture has created, you know, so many opportunities in the Bay Area, but I do worry about with AI, and I have a community in my district called Pleasanton. It is one of the wealthiest communities in America and you have heard of it.

I have other places in my district, like San Lorenzo and Hayward and Union City, and they have some of the poorest communities in the country with schools that don't have enough resources and those kids have dreams as big as kids in Pleasanton. So I just fear that at, you know, a child's earliest days in schools that there are going to be two classes created: those who are given access to AI in their classrooms and those who are not.

So what can the private sector do because you are often, really, some of the best solutions out there to partner with school districts to make sure that you are imparting your knowledge and skills on places that need it the most, recognizing that you are going to have a need to recruit talent down the track as well.

Mr. AMLANI. Sure. Thank you so much for the comments and questions, Congressman. Obviously, this is a pretty personal issue with me, but I think with regards to actually allowing people to have access to the technology and AI in particular it's interesting the way that AI is actually democratizing itself and it's making itself available to everybody.

It's as much of a concern to make sure that actually everyone has access to it and is actually able to have these tools but also people that have gone through large universities and master's degrees and Ph.D.'s now a lot of that content and knowledge is available at people's fingertips who have never gone through any of those programs.

So, you know, with different AI tools that are now available at people's fingertips you can now code. You can now write apps. You can now create content. You know, I've got my 12-year-old creating music right now.

This type of democratization of the AI capabilities is both an opportunity but also a massive threat. It really does upskill many cyber criminals around the globe to be able to attack systems, people that are not as well-off potentially and would love to have the ability to be able to create malware that could potentially create a ransom payment.

So those types of opportunities to be able to educate the youth and make sure that they know how to use it responsibly and for the right aspects are something that I think our society needs to embrace and do a lot more of.

Mr. SWALWELL. OK, thanks.

Thanks again, Chairman.

Chairman GREEN. The gentleman yields.

I now recognize Mr. D'Esposito, the gentleman from New York for 5 minutes of questioning.

Mr. D'ESPOSITO. Well, thank you, Mr. Chairman, and thank you for taking the committee in this direction. I think that it is an issue that really affects every corner of the United States of America and, obviously, our world and has real promises for the future.

Just last week during police week I chaired an Emergency Management and Technology Subcommittee hearing with the Law Enforcement and Intelligence Subcommittee hearing about the use of drones in the first responder world.

We heard a lot about the expanding field and how law enforcement agencies are utilizing drones to assist them in doing their job. I have to say as someone who spent a career in the NYPD it was, it was good to hear and promising that they are embracing technology about how to handle the issues that are plaguing so many cities across this country.

Obviously, as we embrace technology and as the field expands, we meet challenges and we find challenges so listening to all of you speak about the power of AI to assist the United States from attacks from our enemies, it seems that there may be a space for AI in these drones.

So generally speaking, any of you could answer, is AI already being used in drones either by those in law enforcement, the Government, or privately?

Mr. DEMMER. Congressman, thank you for the question. Being in a related field with doing wall-climbing robots primarily, I can say that AI is useful for, you know, using these smart tools properly, everything from localizing data, you know, ensuring that the data point is synched to the location on a real-world asset, to processing millions of data points, or in this case visual images.

We heard a little bit earlier, you know, drones being used as well to secure the border. So there are definitely applications here for that there.

Mr. D'ESPOSITO. Yes, and you mentioned data, so, obviously, drones are utilized by law enforcement to collect that data, whether it is audiovisual, location data, GPS, among others. So that information that is collected needs to—you know, we need to make sure that it is collected correctly and obviously kept private.

So is there a role that AI can play in ensuring that this information remains secure and doesn't give the bad guys access?

Mr. DEMMER. Absolutely, and I'd defer to, you know, my fellow witnesses here on specific policy recommendations for cybersecurity. But, you know, Gecko collects data, you know, massive amounts of information on the physical built world and we take, you know, very seriously the responsibility of securing that data, you know, following requirements like NIST 800–171, NIST 800–172 for these standards of securing the data. You know, also providing training to the entire work force so that they know how to properly handle any type of information or Classified information.

Mr. D'ESPOSITO. Do any of the other witnesses have recommendations with regards to that?

Mr. SIKORSKI. Yes. I could just add that, you know, securing the models, the data that's used to build them is critical. One of the things we deal with the most when doing incident response, especially, you know, ransomware attacks have actually shifted. They no longer encrypt the files on disk anymore. They just focus on stealing data and then use that to extort victims.

So securing the crown jewels of data, which is what most entities have, is paramount.

Mr. D'ESPOSITO. During the—I am sorry, Mr. Amlani, did you have something?

Mr. AMLANI. Sure. This is at Defense Innovation Unit for the autonomous systems portfolio part of my role years ago was actually to manage autonomous systems within drones. I think one of the biggest concerns is actually Chinese-made technology within drones and making sure that we create a list of different drones that people could potentially use in law enforcement and other avenues to make sure that we have a safe list of drones and which is something that Defense Innovation actually did create.

Mr. D'ESPOSITO. So that is actually what—you are leading into my next question. It was almost like we planned this out. So part of the conversation that we had last week from the NYPD was the fact that they currently utilize Chinese technology in their drones and they are working to eliminate them from the fleet because of the issues and the concerns that we have.

My colleague from New York, Ms. Stefanik, has introduced legislation recently that would help law enforcement make sure that they only purchase American-made technology, American-made drones.

But, obviously, those Chinese drones are still in our atmosphere, are still being utilized by first responder and law enforcement agencies. So just quickly, how can AI help us mitigate the threats that they pose?

Mr. AMLANI. There's also a significant amount of work being done by Defense Innovation Unit and other agencies on mitigation of drones and counter-drone work. So AI used for counter-drone work is also another way to be able to mitigate those.

Mr. D'ESPOSITO. Excellent.

My time has expired. Mr. Chairman, I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the gentleman from California from Los Angeles, Mr. Garcia. You are recognized.

Mr. GARCIA. Thank you, Mr. Chairman. I appreciate you holding this hearing.

I want to thank all of our witnesses for being here as well. It is truly amazing how fast AI has evolved and continues to evolve every day.

It used to be something, of course, a lot of us would read about or see in movies and read about in science fiction novels, it has changed so much and just the progress of AI in just the last 6 months to a year has been startling.

But also, I think, shows the promise of what AI can actually do in our lives and how we can also improve our lives as Americans and as a world.

Like a lot of folks here, the concerns as it relates to our own security, our own homeland security challenges we have here in this country, but I also want to focus on the challenges it faces to our own democracy and our elections process. A lot of my colleagues have brought that up in the past and there are bills to address that, of course, here in the Congress as well.

You know, just in the last 24 hours DHS issued a warning ahead of the 2024 elections of threats that AI poses to our very elections. Earlier this year the World Economic Forum announced that AI threatens and continues to threaten global democracy, not just here in the United States but across the globe. This assessment was actually echoed just last week by our own intelligence community.

The DNI intelligence officials have testified in the Senate that since 2016 when Russia first tried to meddle in our elections that the threats are happening from foreign actors even more. So as we know today, Russia, China, Iran, others competing to influence not just their own countries but what is happening in our own elections here in the United States. That is actually a very danger to all of us and a concern for us as well.

Now this past January, we know that voters in New Hampshire were exposed to one of the most high-profile recent cases of AI. We know that there was a robocall, for example, impersonating President Joe Biden telling people not to vote.

That attempt, of course, was identified, stopped, and investigated, which I think we are all very grateful for. But we can see that those types of efforts could cause enormous havoc, especially in elections that were close if they were targeted in States or in communities across the country.

We already know that there has been unsuccessful and successful attempts to undermine our elections in 2016 and 2020, and folks are trying to do it again in 2024. So the rise of AI, deep fakes, and other technology is very concerning, I think, to the Congress and to all of us.

I am also especially concerned because, well, one of both the advantages in the United States is that we have a lot of—our elections are decentralized. Our elections are not run generally by the Federal Government. They are run by States, counties, towns, cities, oftentimes small communities without a lot of resources or the technology to know how to actually deal with kind of the oncoming, I think, wave of AI attempts to actually meddle in all of these elections.

So I am really concerned about how these smaller agencies, these city clerks actually are able to take on AI and have the resources to do so.

We know that the new DHS Artificial Intelligence Task Force, which is coming out of Homeland Security, which I think is really important, but this is a huge, I think, responsibility of this committee is how we provide and get assistance to these clerks and county recorders across the country.

Mr. Laperruque, I know that CDT has done a great, good deal of examining some of these risks. What additional safeguards do you think need to be put in place as it relates to this election piece? How can Congress better support all of these election organizations and officials across the country that have a decentralized system? How are they supposed to get support? That is, I think, very concerning.

Mr. LAPERRUQUE. As you were emphasizing, the decentralized nature of our elections, which in some ways provides a lot of assets, is also a significant challenge when you're facing threats like this.

So we, unfortunately, over the last decade have built up a robust network of Federal entities that provide support for election security from things such as cyber threats.

I think we should supplement that by having those same entities serve as means for highlighting AI threats, whether that's of a specific type of attack or a misinformation campaign that's going around, using that to disseminate information, but also for more general awareness and education that can be brought from that small set of Federal entities and disseminated outwards to that broad network trying to educate about here are the types of AI technologies.

Here's how they might be used for everything from trying to use AI to create spam FOIA requests to overload your office to building up fake materials about polling information to using AI for spear-phishing.

Mr. GARCIA. Could I also just finally, I think what is—even though we have for, you know, our elections obviously for President or U.S. Senator, these are Federal elections, but they rely on data from local towns and counties and registrars that just send their information and their voting information up through the process through the State and then eventually, of course, the States will certify elections.

So the real concern is that you can micro-target, of course, precincts. You can micro-target small towns and cities with these AI disruptions that can have real impacts in certain States to Presidential elections. I think that is something that I think we have to really consider and think about as we move forward and how we get these small towns and city clerks the technology but also the education that is needed to take on this these deep fakes and AI concerns.

So with that, I yield. Thank you.

Chairman GREEN. The gentlemen yields.

I now recognize the gentlelady from Florida, Ms. Lee, for 5 minutes of questioning.

Ms. LEE. Good afternoon. Mr. Sikorski, I would like to go back to your testimony where you mentioned that our cyber adversaries are utilizing AI to really enable some of their malicious behavior, like creating more sophisticated phishing attacks, finding new attack vectors, enhancing the speed of lateral movements once they do intrude upon a network.

I am interested in hearing more about how we are using machine learning to build and enhance our cyber defenses against these kinds of attacks. You mentioned in your written testimony precision AI, some other tools including some revisions to how the SOCs are operating.

Would you elaborate for us on how machine learning can enhance our cyber defenses?

Mr. SIKORSKI. Yes, it's a great question. Actually Palo Alto Networks and myself have both been involved on this machine learning AI journey for over 10 years. This isn't while ChatGPT and other technologies like that have gotten really popular really quick, we've been leveraging that type of technology for quite some time.

Myself specifically on, you know, malware, anti-malware technology to be able to detect malware on a system and so we've been training models to do that. We've been in it for quite some time and that detects sort-of variation in what we're seeing and making sure that variants of malware that come out will be stopped due to that training.

Then there's also the idea of sort-of leveraging AI to get rid of the noise. That's really the more recent evolution that we've been focused on at Palo Alto Networks where we're trying to say everybody's inundated with all these tools.

You know, go back to the Solar Winds example.

I did numerous incident responses to that after, you know, that came out. I went on to corporate networks and one of the big problems that they had was they actually detected the attack. They detected the malware being dropped on a system. They detected the lateral movement, but they didn't know it was there because they were flooded with so much noise.

So what we're doing is we're taking our technology and very much focusing on how to put these alerts together, reduce the amount of information so that the brains of the analysts, who by the way are getting burned out by having to look at so much data that makes no sense to them, instead it gives them a chance to zero in on the attack, figure it all out, and then actually move the needle.

Ms. LEE. You also mentioned in your testimony at a point about the unintended consequences of disclosure, and I would like to go back to that, particularly raise a concern that public disclosures that require information about how we are using AI to train and defend networks that requiring disclosures of a certain type could unintentionally create a roadmap for the cyber adversaries and reduce our overall security.

I am interested if you were a policy maker how would you balance disclosure requirements with not alerting our adversaries to the type of information that we don't want them to have?

Mr. SIKORSKI. Yes, that's also a great question. I think about it's all about the, like, what is your end goal with respect to the AI that you're trying to get to customers or to protect the network? I think you've got to think about the risk level involved there and think about the tradeoff, right?

The more that we regulate things and think about what's there and really put a lot of pressure on oversight it could slow down the innovation and the protection. I think it's the appropriate thing to do when we're talking about somebody applying for a home loan or something like that, thinking about every step of the security process with that.

I think when we start to talk about cybersecurity we've got to focus on what is the data and is the data, the ones and zeros, the malware, the detections to be able to eliminate attacks and how important that is to make sure that we continue to make a difference with the technologies that we're building on the cyber war that we're all out there fighting day in and day out.

Ms. LEE. You also mentioned, that reminds me, of the concept of secure-by-design. I know it is something that we need to be contemplating as we analyze internally what to regulate it and in what manner.

Share with us, if you would, a little bit more about secure-by-design and what that should mean to us as Federal policy makers.

Mr. SIKORSKI. Yes, I think it goes back to the point that AI is here to stay no matter what any of us do, right? Like, it's coming and it's sort-of like the internet, right, but we didn't plan security into the internet. We didn't plan security into all of the applications and everything that was built out.

Instead what we're stuck doing, and especially comes up as a cybersecurity company, is, you know, we missed out on an opportunity to build things in a secure way. That's where when it comes to securing-AI-by-design you think about what are you building, how are you building it? What are you pulling in from the supply chain into that build? How are you protecting the application as it's running? How are you protecting the models, the data, everything as it's actually flowing out to customers or otherwise?

I think that's where a really big focus on building things in a secure way is really important.

Ms. LEE. Thank you.

Mr. Chairman, I yield back.

Chairman GREEN. The gentlelady yields.

I now recognize Mr. Menendez for 5 minutes of questioning.

Mr. MENENDEZ. Thank you, Chairman, and thank you, Ranking Member, for having this hearing.

Thank you to all the witnesses. I first want to start and build off some of the questions that my colleagues have asked about training our cybersecurity work force and first want to acknowledge Hudson County Community College, which is in New Jersey's 8th Congressional District.

It is designated as a National Center of Academic Excellence in Cybersecurity by the NSA. They were recently awarded $600,000 to expand their renowned cybersecurity program which is getting more women into the cybersecurity field, so incredibly proud of the work that they are doing.

Mr. Sikorski, thank you for emphasizing the need to educate and train our cyber work force. I am wondering in your experience what are you seeing as the most prominent barriers to participation in the cyber work force?

Mr. SIKORSKI. I think there's a few parts to that. I think the first is desire. I think that getting people at a much younger age, you know, focused on getting excited about these technologies and wanting to get involved in what's happening.

It goes back to what we discussed earlier which is how do we make sure they have proper access and actually are talking about AI and cybersecurity at a very early age?

Then I think that to the point of what's happening in your district is very focused on how do we build the university system such that they're really feeding the engine of all of these cybersecurity work force shortage jobs that we need to actually fill?

So I think, you know, and working with industry to make sure that they're lining up for the jobs because, you know, a lot of cybersecurity companies actually struggle to find talent to hire into these jobs which go into, you know, securing networks around the world, collaborating with CISA, and other things that we're doing.

There's just not enough people to pull from there.

Mr. MENENDEZ. Yes, because across public-private sectors everyone is looking to enhance their cybersecurity capabilities which includes adding cybersecurity professionals, whether it is the Port Authority of New York and New Jersey or whether it is a private entity that is concerned about these issues.

Just sort-of quickly following back, you mentioned a desire at a younger age for people to engage in this field. I believe you are an advisor to Columbia's cyber student organization. Are you seeing anything sort-of in that student demographic that draws them to cyber that maybe we should be sort-of using to highlight and amplify at a younger age?

Mr. SIKORSKI. Yes. That's a great question. I think that one thing I think about is the gamification of it.

Mr. MENENDEZ. Yes.

Mr. SIKORSKI. When I think of myself personally I wanted to be a video game programmer originally because that was really cool back in the Nintendo days, right? I had the tech skills for it. But then once I realized that, you know, cybersecurity is like this, it's good-versus-evil kind of situation going on in the real world and it's only going to get bigger, I started to get really excited.

Then there's hacking competitions and like, you know, driving that into getting people to participate more because of the fun that can be had and the team building that could be had working toward that.

That doesn't really exist out there but that's what actually happens at Columbia University. There's a cybersecurity club where they focus on that. They go to competitions together and it rallies them into a common goal. I think those types of things are great.

Mr. MENENDEZ. That is great. I appreciate it.

I am going to shift real quick to Mr. Demmer. In your testimony you touched on how AI can be used to better secure physical infrastructure and you specifically note the collection of high-quality, high-quantity data.

I also sit on the Transportation Infrastructure Committee. We are overseeing the major investment that is being utilized by the Infrastructure Investment and Jobs Act, which is building our future infrastructure.

I was commissioner of the Port Authority of New York and New Jersey. One of my favorite projects was Restoring the George where they went through and cables, and it was a completely intricate project but necessary.

As we think about investing in our infrastructure so we don't have to make these huge investments of replacing our existing infrastructure, how could the use of AI and the data collection that you touch on be used to better upkeep our existing infrastructure?

Mr. DEMMER. Thank you, Congressman. This is, you know, something we care deeply about. Of course, protecting the infrastructure we have today, capturing the right dataset so that we can ensure that they are here for us when we need them not vulnerable to, you know, just wear, old age, or some external threat.

But increasingly, we also see the opportunity with these datasets to help us build more intelligently in the future. So as we bring new systems on-line how do we instrument them in ways where we can do that modernization and telemetry of what's going on with that equipment so that we don't have sort-of the failures or the vulnerabilities? Hopefully lower that cost of maintenance because two-thirds of the cost of critical infrastructure is usually consumed after the initial build.

Mr. MENENDEZ. That is right. What type of dollar amount investment could the Federal Government make to quickly scale up this technology and put it to use?

Mr. DEMMER. Yes. So there are, you know, very much, you know, technology-ready solutions out there for national security and there are ways that, you know, I'd love to follow up with some guidance on that in terms of programs that could be utilized to help bring those technologies to the forefront and accelerate the adoption of them, whether it be investment in hardware technologies, as well as, you know, ensuring that the policy side has recognized that not all solutions are created equal.

Today we do a lot of things that seem, seemingly placate the ability to think that we have a handle on what's going on, but it's actually woefully inadequate in terms of how we're actually managing, you know, and maintaining.

Mr. MENENDEZ. Sure. I would appreciate to continue this conversation, but I am woefully out of time. So I yield back.

Chairman GREEN. The gentleman yields.

I now recognize the gentleman from North Carolina, Mr. Bishop, for 5 minutes——

Mr. BISHOP. Mr. Chairman, I yield my time to you.

Chairman GREEN. Thank you. A quick question on the creating a sense of security for the public on AI. There is all the fear that is out there and are there requirements that we can place in the system that would give people a sense of security?

I mean, kill switches, always having a person in the system, what are some things that we can do give the public a sense of security that we are not going to create, you know, The Terminator or something like that? Anyone? You are smiling.

Mr. LAPERRUQUE. I'd say human review and control is one of several factors that's critical for something like this. Again, I think you need strong principles to ensure responsible use all the way from creation to what data you're putting into systems and what systems you are using AI for to what data you're taking out and how you're using it as you said, you know, for human review.

One of those steps on this sort-of on the outside is there should be human cooperation for AI results. It shouldn't just be AI making its own decisions.

We have to know how reliable AI is in certain circumstances. Sometimes it can provide small bits of insight, sometimes it can be very reliable, sometimes it gives a degree and you have to treat it with a bit of skepticism. But also maybe it provides a bit of value along those lines, not just human review but specially-trained staff. That's why it's so important for folks that won't just overcome a general automation bias.

That's the tendency for individuals to always just assume that automated systems tend to work better than humans. That's been documented in many cases, but you need to understand what type of biases or what type of liability you might want to apply to any given AI system in any situation.

Chairman GREEN. Mr. Amlani, Mr. Laperruque has said some negative things about facial recognition earlier, I think if I heard him. Maybe not negative, but concerning and the fairness in the use of it against large groups, population stuff, law enforcement.

What are your thoughts on the reliability of facial recognition and since this is your field, is there something? I am aware in my district of a company that has the use of the three-dimensional vasculature in the hand, for example, which apparently according to them hasn't failed, but facial recognition has failed.

So what are what are your thoughts on it? Because identity, I think you are right, it sort-of begins and ends with being able to make sure the person is the person in the system, to make sure that it is. So what are your thoughts on that?

Mr. AMLANI. Thank you, Mr. Chairman. This is actually a really important question from even going back to your prior question about building confidence in individuals and systems in AI. I think it ties to that as well, which is fundamentally, you know, post-9/11 after the terrorist attacks, one of the steps that we did is we actually Federalized the work force and created TSA.

Having Federal agents at the checkpoints actually made people feel safer to get back on airplanes again. That used to just be a private contracted work force paid for primarily by the airports and the airlines, but by having Federal agents there it made people feel more comfortable. So these steps are really important to be able to put into place.

People do not feel comfortable right now with identification and authentication steps that are necessary right now to access systems. Passwords are antiquated. People forget passwords. The most secure place to actually store passwords, according to all of the major cybersecurity experts in the field right now, is actually in a personal book that you write with you because nobody overseas actually is trying to steal your personal book of passwords. They can access your systems. They can steal centralized places where you store passwords, but your book of passwords is something that they have very difficult access to to receive.

So leveraging better authentication mechanisms builds confidence in digital tools and capabilities. People have become very comfortable with face ID to be able to actually secure their systems. People have no confidence in what Ranking Member Thompson mentioned with regards to on captchas, right, and other silly systems like one-time passcodes that get sent to your phone, which are very easily compromised.

So giving people that confidence with facial matching and facial recognition and facial verification is an important component.

Chairman GREEN. If I can jump in now because in the time remaining I have a quick question for Mr. Sikorski. Data poisoning, how big of a threat is that for the AI systems that are using that data to make very quick decisions particularly in the defense world? If we need to go somewhere else to have that conversation we can postpone it until then, but if you could just real quickly share a few concerns about that, if you have any.

Mr. SIKORSKI. Yes. I think it goes back to the secure-AI-by-design, right? As we're building out these applications how are we securing that information? How are we securing the models themselves that make the decisions as well as the training data that goes there?

There is a lot of research and a lot of thought about what attackers could do if they could manipulate that data, which would then in turn not even necessitate an attack against the technology itself. It's an attack against the underlying data with which it's trained with. That's definitely a concern that needs to be taken into account and built into as the technology is being built out.

Chairman GREEN. Thank you. I yield.

Mr. Goldman, the gentleman from New York, is recognized for 5 minutes.

Mr. GOLDMAN. Thank you, Mr. Chairman.

Thank you all for being here. The 2024 Worldwide Threat Assessment warns that our most sophisticated adversaries, Russia, Iran, and China, see the upcoming Presidential election as an opportunity to sow disinformation, divide Americans, and undercut our democracy.

Many of our law enforcement and intelligence agencies have confirmed that they are also seeing upcoming threats. Of course, it is not abstract.

We know Russia used social media and cyber to interfere in our election in 2016. We know that Iranian actors posed as Proud Boys in an on-line operation aimed at intimidating voters in 2020. Just recently, we learned that China is experimenting with AI to enhance their influence operations.

Within the Department of Homeland Security, CISA is charged with protecting the security of our elections.

Mr. Sikorski, I know you work closely with CISA on some of these issues and I would love just to ask you a relatively open-ended question, which is how is CISA prepared or how is our Government writ large prepared to address the use of AI by foreign adversaries to undermine and interfere in our elections?

Mr. SIKORSKI. That's an excellent question as we want to have a very secure election, obviously. I think CISA is doing a great job with the JCDC, which is the collaboration with private industry to work with us, Palo Alto Networks, and many other private entities on thinking through, like, what are we actually seeing in the threat landscape?

So one of the things I'm tasked with as running the Threat Intelligence Division at Palo Alto Networks, is how do we take all of the information that we're getting from other private entities, from government agencies around the world, bring that all together and then share that back with the Government itself to say this is where we're seeing these threat actors go, right? Whether it be what China is up to today, what Russia is doing in the war in Ukraine, staying on top of those threats and finding the new ones.

For example, we saw, you know, a novel attack of how Russia was sending emails, phishing emails, to Ukrainian embassies and actually making that discovery and showing how that actually went down. So that hyper collaboration is definitely going to move the needle.

Mr. GOLDMAN. One of the biggest threats is deep fakes which are, we know, our intelligence agencies said that they had spotted Chinese and Iranian deep fakes in 2020 that were not used, but the FBI has recently identified that recent elections in Slovakia were impacted by the use of deep fakes.

How prepared are we to prohibit or prevent the use of deep fakes that might have a significant impact on our election?

Mr. SIKORSKI. Yes. So I think what we've seen with AI it really lowers the bar for attackers to be able to generate believable communications, whether that's emails like I talked about earlier with phishing, whether it be voice or even a deep fakes technology.

So I think that that lowering of the bar makes it a lot easier to make believable things that they're going to select. At Palo Alto Networks we're not hyper-focused on, like, you know, eliminating, you know, deep fake technology, and I think that that impact of inauthentic content is really concerning and something we need to explore.

Mr. GOLDMAN. Anyone else have any insight into this?

Mr. AMLANI. Yes. At iProov we are actually obsessed with detecting deep fakes. That is actually what we do.

We use screen lighting from a cellphone screen or a desktop screen that reflects against live human skin, calculating 3D geometry, making sure that it's a live human being, including skin translucency, all simultaneously while you're actually recording a video or doing a biometric match and verifying that it's a live human being and the right person at the right time, you know.

With being there at the creation of the video is an important component that you can then tag the video and verify that it's, in fact, not a defect.

Mr. GOLDMAN. Are you coordinating with CISA on this?

Mr. AMLANI. No. We have not been asked by CISA.

Mr. GOLDMAN. Mr. Laperruque.

Mr. LAPERRUQUE. Yes, beyond just the cyber risks, I mean, deep fakes is something that our elections team and misinformation in general has highlighted that one of the risks is the liar's benefit. That, you know, in addition to misinformation going out there and this is something that when you're evaluating truthful information someone could just say, no, that was just a deep fake. No, that was just misinformation.

It's not just the initial itself misinformation. It's trying to create an entire ecosystem of uncertainty so it's just that's, you know, to emphasize why it's such a significant threat and why we need to make sure that we have clear information and ways of trying to debunk this that are reliable.

Mr. GOLDMAN. Mr. Chairman, I know that you and—oh, he is not here, but you and many of the Members on this committee are concerned about election security. I would just urge you to encourage some of your colleagues who are trying to interfere with law enforcement's efforts to coordinate election security and prevent election interference with the cyber companies who through which the adversaries do try to influence.

I hope that we don't see any more Members of the Republican Party trying to cut funding in CISA and that we work closely with CISA to make sure that our elections are safe. I yield back.

Mr. BRECHEEN [presiding]. Mr. Goldman yields.

The Chair now recognizes Mr. Crane from Arizona for his 5 minutes.

Mr. CRANE. Thank you, Mr. Chairman. I realize that this hearing is about utilizing AI to bolster homeland security. I want to bring up an interesting meeting I just had in my office before coming to the committee.

I was with one of the largest tech companies in the United States and arguably global companies, and they were talking about major cybersecurity attacks that they are seeing.

I was told that they used to see attacks in the range of tens of thousands a day. They are now seeing attacks to the tune of about 150,000 a day.

Mr. Demmer, Mr. Sikorski, is that consistent with what you all are seeing and hearing in your space as well, an increase in cyber attacks?

Mr. SIKORSKI. Yes, we've—yes. That's a great question. We've actually seen a great increase in cyber attacks and the number of pure attacks that we're stopping on a per-day basis across all of our customers, which is 65,000 customers, is, you know, in the billions, right?

Now, actual net new it's in the millions, but that still gives you a sense of, like, you know, how many new attacks are going on. Then we see the cadence of ransomware attacks and extortion continuing to increase as all these ransom gangs have evolved.

Mr. CRANE. This company also told me that not only are the numbers of attacks on a daily basis increasing drastically, but they also said the brazenness of some of these foreign actors is becoming more and more hostile and increased as well. Is that something that you all can verify that you are seeing as well?

Mr. SIKORSKI. Yes. I think the days of a ransomware attack where they just encrypt files and you're just paying for a key, we actually miss those days because now they're stealing the data and harassing our customers to get ransomware payments.

So they're taking that data which has their customer information, patient data in some instances, threatening to leak that out and really going to what I call a dark place of, like, the level of harassment they're willing to go to.

They're sending flowers to executives, and they're even going after companies' customers pretending to spam them as the company when, in fact, they're the threat actor harassing their customers and then leading to getting the payment that they're after.

Mr. CRANE. My real question to you guys is what do you attribute this stark and drastic rise in aggression and the amount of cyber attacks that we are now seeing against our own corporations and also our infrastructure?

Mr. Demmer, I am going to start with you.

Mr. DEMMER. So thank you, Congressman, for the question. You know, my expertise really lies on the physical infrastructure, the critical assets that we help maintain and protect. I can say that, you know, the threats are arising on our critical energy systems, on our infrastructure like bridges and roadways and dams.

Although we haven't seen, you know, the pace of attacks that we are seeing on the cyber side, it is a real vulnerability and a risk as our infrastructure ages and has more vulnerabilities. So it's something that our company is looking at.

Mr. CRANE. What about you, Mr. Sikorski?

Mr. SIKORSKI. I think the threat actors, specifically in crimeware and when we talk about ransomware have become a business where it's actually not the same hacker who's breaking in and then doing the ransomware and everything else.

It's actually one group breaks in and then they sell that access on the dark web to ransomware gangs who are almost like franchises like McDonald's or something where they pop up. They have a reputation score of how likely they're there to do what they say they're going to do about giving the data back.

That enables them to build the relationships and get the access they need. So this almost it's operated like a 9-to-5 job for some of these ransomware operators.

Mr. CRANE. Let me ask you something more pointedly. Do you believe that some of these nation-states and some of these foreign actors, do you think that they sense weakness here in the United States? Do you think that has anything to do with it?

Mr. SIKORSKI. So I don't think that I could speak to if they sense weakness or not. I think it's more an opportunistic thing from what I see. We've seen them leverage vulnerabilities——

Mr. CRANE. Well, did those opportunities—sir, did those opportunities, were they not present a couple of years ago?

Mr. SIKORSKI. I would say those opportunities have always been present. There's always been vulnerabilities in systems, however, the availability and opportunity for them to figure out how to get in has increased. They are better enabled and now that they're operating in this, in this model and it makes them more efficient and able to pull out overt attacks.

Mr. CRANE. What do you think we could be doing? Do you think we are doing enough offensively to make sure that individuals that would utilize these types of technologies to attack corporations and U.S. infrastructure—what do you think we could be a better job of doing to make sure that they pay a heavy price if they are going to carry out these type of attacks against our country?

Mr. SIKORSKI. Yes, that's a great question. I think when I think about, you know, I'm not a policy maker as far as thinking what's the best stick to have when it comes to dealing with the cyber threat.

One of the things that I'm always focused on is on the defensive side, right, and how do we make sure we're doing everything we can to secure. Then opening all the lanes for sharing on the threat intelligence front, which is big steps and strides we have made in recent years, the last few years.

All of this collaboration that's happening is moving the needle. I think that'll help a lot us staying, you know, in front of what the adversary is.

That being said, we're in an arms race right now on AI, right? The defenders need to win here because one opportunity we have is we could use AI to remove all those vulnerabilities I was talking about before the threat actors can use AI to find them.

Mr. CRANE. Thank you.

Thank you for the extension, Mr. Chairman. I yield back.

Mr. BRECHEEN. The gentleman being last gets some extra grace, as did Mr. Goldman. The gentleman yields.

I now recognize Mr. Kennedy from New York for his 5 minutes of questioning.

Mr. KENNEDY. Thank you, Chairman, and thank you to the Ranking Member.

Thank you to the panel today for your testimony. We are hearing a lot about advancements in AI and the upcoming election. It is a historic election. We want to make sure that it is secure.

As November approaches, there is more and more concern about those that would seek to undermine our election. As a matter of fact, just last week a report from the Department of Homeland Security warned, and I will quote, "As the 2024 election cycle progresses, generative AI tools likely provide both domestic and foreign threat actors with enhanced opportunities for interference by aggravating emergent events, disrupting election processes, or attacking election infrastructure."

So I worry about the rapid advances having an impact on the election as we are discussing here today. The Cybersecurity and Infrastructure Security Agency is responsible for election security.

Mr. Laperruque, how can this agency best support election officials and United States voters so that they can trust the authenticity of the content that they are seeing when they see information on-line?

Mr. LAPERRUQUE. Well, as I said before, I think this is an area where we can learn a lot of lessons from what we've taken in cybersecurity space over the last 5 to 10 years using these type of Federal agencies to distribute information out to the huge range of local election administrators, as well as the public.

That comes from both providing education about how these technologies work, how threats work, what to be aware of, as also—as well as information about specific threats if there is something on our monitor, some sort of common deep-fake technique, some sort of new type of attack on providing information in that field.

It's something where because our election system is so decentralized and because there is a lot of information out there sort-of acting as that hub of getting out good and useful information and warnings can be very important.

Mr. KENNEDY. What do you foresee as a role for the Cybersecurity and Security Agency in authenticating content on-line in regards to the upcoming election?

Mr. LAPERRUQUE. I think that would be a much more challenging question if we're talking about just content from, you know, any layperson as opposed to a message that may be targeted at an election administrator.

You know, that's something that our elections team, which is separate from my work, does a lot of research into so I would encourage, you know, continued work with them. They're always happy to provide thought and detailed research into this space.

Mr. KENNEDY. Great, thank you.

Then I know Chairman Green earlier mentioned, you know, his community, but I want to plug the University of Buffalo which established the U.B. Institute for Artificial Intelligence and Data Science to explore ways to combine machine's ability to ingest and connect in 2021. Just this past year, the New York State budget included $275 million for the University of Buffalo's new AI center.

So, Mr. Amlani, when you are searching for universities with your 15-year-old you should look at Buffalo and the engineering school that they have there right in the heart of my community.

But how can we better harness the institutes of higher ed, especially our public institutions, for getting at this cutting-edge technology? While they are training up our youth in this new technology how do we make sure that they are developing it in a safe way regarding AI?

Mr. AMLANI. So thank you so much for your question, Congressman. My son and I would love to come to Buffalo. We would also love to be able to visit Niagara Falls.

Mr. KENNEDY. You are always welcome.

Mr. AMLANI. Thank you. Fundamentally, I think there is a level of distrust in some of the AI content created and much of that distrust is not knowing who or where the content came from. So it comes down to identity, properly identifying the creator and properly verifying the content has not been tampered with after it was created by the initial creator.

So making sure that you're able to identify the initial creator is a very important component on trusting all of this content and also for intellectual property concerns and other aspects of things that we've already discussed here today.

So using proper identification tools, things that can verify that it's the right person, it's a real person, and it's right now to allow the individual to have ease of use to be able to identify themselves and verify they are who they say they are and the content is coming from them.

Mr. KENNEDY. Thank you.

I yield my time.

Mr. BRECHEEN. The gentleman yields.

I now recognize myself for 5 minutes. So for the purpose of, you know, this committee I think a lot of the questions are centered around the border and how AI can help us be able to identify fraud and also protect entities within the United States.

That is where I want to go here initially. The ability of your company to help bolster border security, for those of you that are representing the free market, I really, Mr. Sikorski, you had alluded to, I have got some information here where AI-powered copilots, my understanding it is a natural language assistance that can yield you guys state, you know, multiple operational advantages.

I am actually curious as to when we are doing our initial credible fear interviews, asylum claims, if our border security officials can utilize that tool to better inform the cases of the future so that as people are being coached for those interviews with which can be fraught, you know, a language barrier can exist and they can be told to say certain keywords.

Have you all or anyone on the panel aware of how we can make sure that we can get to the depth of fraud for our officers to be able to use AI to be able to get past a language barrier that can be used as a defensive mechanism to the benefit of those who are applying help us get to the truth of the matter?

Mr. SIKORSKI. Yes, that's a great question. I think I'll take from my experience helping to create that technology at Palo Alto Networks. So when we say copilot what we mean is you have a human who's using technology to find new threats, right? That's what we sell.

But it's very difficult to use so what we end up doing is we built these technologies called copilots for our products so that users can engage very quickly to ask questions just, you know, and then the AI will process the question and give them the answer that's there so they don't have to figure out all of the complex complexities of our product.

I think what you can do is you can take what we've done in that capacity and apply that to a use case, like where you're talking about, where you can say they get a copilot and they're paying attention to what they're collecting, what information, and the AI maybe says to them, hey, you know, I saw it differently than you saw it when I feed all this in and put it against my model.

Then you could put the two side-by-side and it's sort of like Iron Man where you put on the suit and you're more powerful than you were before. That's sort-of one area I would think to go into.

Mr. BRECHEEN. So to elaborate, if I am understanding you correctly, you do think that CBP officials could be empowered in those moments to help inform the case? But I am assuming there is also the defensive mechanism that someone crossing illegally with credible fear asylum claim wouldn't be fraudulent could also use that technology to time delay, read the question and then I am assuming the technology is moving there where they can get a response to help their case also that is AI-generated.

Mr. SIKORSKI. Yes, I'm not—I'm definitely not an expert on, you know, the border and how those policies are to figure out, you know, what the best way is on immigration and other things. However, the thought processes, the types of things we're doing with AI to enable customers or prevent cyber threats could. The model is similar for really anybody who's collecting data to make better decisions that they might not otherwise do by themselves.

Mr. BRECHEEN. Let me move on. The rise of AI, the significant question about, you know, concerns, Constitutional, elections. AIs can be very dangerous when we are dealing with China, social credit scores, and the ability to have facial recognition AI-powered that then may produce a different outcome depending upon whether you adhere to the Government's positions or not.

So there is a real fear and it is a credible fear out there for those of us that think this could be used or weaponized against a nation's citizenry.

I want to ask from your perspective, the significant concerns you have regarding the AI of the future. If anybody wants to talk about election fraud, specifically candidates that can be created to look like they are saying something that they are not actually saying and how that could be generated, the ability for a user and I am not talking about Government regulation here but for a user to have a fact check, something that could be encrypted where I could have the ability to determine whether or not that was created or if that is an actual video?

If anyone wants to respond to that?

Mr. AMLANI. Sure. I think the identity of the creator is actually a very important component up front, Mr. Chairman, Mr. Congressman. I believe that right now that is not actually associated with most of the videos.

It is shared openly. It is shared on open sites and you can never really tell who created the original video. If you had the ability to be able to do so at least you would have some confidence that the video itself was actually created originally by the initial creator.

But there is some watermarking tools and other technologies being used by other companies that there's some investment in that space currently today to be able to assess it.

Mr. BRECHEEN. Interesting.

I want to honor the time here and with that I yield to the gentlelady from New York, Ms. Clarke, for her 5 minutes.

Ms. CLARKE. Thank you, Mr. Chairman.

I thank our Ranking Member in absentia for holding this important hearing.

Let me also thank our panel of witnesses for bringing their expertise to bear today. The rapid advancements in artificial intelligence and cybersecurity represent significant new opportunities and challenges with respect to securing the homeland.

Every day developers are creating new AI tools to better identify and respond to the increasing number of cyber attacks. But while AI is a critical tool in our cyber defenses, it is also still created and deployed by human beings.

AI systems are trained on datasets which often replicate human biases and thus, the bias is built into the very technology created to improve our lives and keep us safe.

For example, AI designed for law enforcement purposes that was trained on historic police or crime data may serve to reproduce or expand existing inequities in policing as those are not an accurate reflection of crime but rather of police activity and crime reporting, which can be fraught with bias.

While artificial intelligence and cybersecurity will remain important elements defending the country, these are not just technological issues but critical civil and human rights issues as well.

To that end, Mr. Chairman, I ask unanimous consent to enter into the record an insightful article on this topic published in *Wired.*

Mr. BRECHEEN. Without objection, so ordered.

[The information follows:]

ARTICLE SUBMITTED BY HONORABLE YVETTE D. CLARKE

THE HIDDEN INJUSTICE OF CYBERATTACKS

By Nicole Tisdale, Wired Magazine, Feb. 12, 2024

Cyberattacks and criminal scams can impact anyone. But communities of color and other marginalized groups are often disproportionately impacted and lack the support to better protect themselves.

Talk about the promise and the peril of artificial intelligence is everywhere these days. But for many low-income families, communities of color, military veterans, people with disabilities, and immigrant communities, AI is a back-burner issue. Their day-to-day worries revolve around taking care of their health, navigating the economy, seeking educational opportunities, and upholding democracy. But their worries are also being amplified through advanced, persistent, and targeted cyberattacks.

Cyber operations are relentless, growing in scale, and exacerbate existing inequalities in health care, economic opportunities, education access, and democratic participation. And when these pillars of society become unstable, the consequences ripple through national and global communities. Collectively, cyberattacks have severe and long-term impacts on communities already on the margins of society. These attacks are not just a technological concern—they represent a growing civil rights crisis, disproportionately dismantling the safety and security for vulnerable groups and reinforcing systemic barriers of racism and classism. The United States currently lacks an assertive response to deter the continued weaponization of cyber operations and to secure digital access, equity, participation, and safety for marginalized communities.

Health Care

Cyberattacks on hospitals and health care organizations more than doubled in 2023, impacting over 39 million people in the first half of 2023. A late-November cyberattack at the Hillcrest Medical Center in Tulsa, Oklahoma, led to a systemwide shutdown, causing ambulances to reroute and life-saving surgeries to be canceled. These attacks impact patients' reliance and trust in health care systems, which may make them more hesitant to seek care, further endangering the health and safety of already vulnerable populations.

The scale and prevalence of these attacks weaken public trust—especially among communities of color who already have deep-rooted fears about our health care systems. The now-condemned Untreated Syphilis Study at Tuskegee, where researchers denied treatment to Black men without their knowledge or consent in order to observe the disease's long-term effects, only ended 52 years ago. However, the study created a legacy of suspicion and mistrust of the medical community that continues today, leading to a decrease in the life expectancy of Black men and lower participation in medical research among Black Americans. The compounding fact that Black women are three to four times more likely, and American Indian and Alaska Native women are two times more likely, to die from pregnancy-related causes than White women only adds to mistrust.

Erosion of trust also extends to low-income people. Over a million young patients at Lurie Children's Surgical Foundation in Chicago had their names, Social Security numbers and dates of birth exposed in an August 2023 breach. The hospital treats more children insured by Medicaid—an economic hardship indicator—than any other hospital in Illinois. Once breached, a child's personal data could be used to commit identity fraud, which severely damages credit, jeopardizes education financial aid, and denies employment opportunities. While difficult for anyone, children from financially insecure households are least equipped to absorb or overcome these economic setbacks.

Economic Opportunity

Identity theft is not the only way cyberattacks exploit hard times. Cyberattacks also go after financially vulnerable individuals—and they are getting more sophisticated. In Maryland, hackers targeted Electronic Benefits Transfer cards—used to provide public assistance funds for food—to steal more than $2 million in 2022 and the first months of 2023. That's an increase of more than 2,100 percent compared to the $90,000 of EBT funds stolen in 2021. Maryland's income limit to qualify for the government's food assistance program is $39,000 for a family of four in 2024, and only if they have less than $2,001 in their bank account. Unlike a credit card, which legally protects against fraudulent charges, EBT cards don't have fraud protections. Efforts to help the victims are riddled with red tape: reimbursements are capped at 2 months of stolen benefits, and only within a specific time period.

Cybercriminals also target vulnerable populations, especially within older age groups. Since the last reporting in 2019, 40 percent of Asian Pacific Islander Desi Americans (APIDAs) aged 50 and older have reported experiencing financial fraud, with one-third of those victims losing an average of $15,000. From 2018 through 2023, Chinese Embassy Scam robocalls delivered automated messages and combined caller ID spoofing, a method where scammers disguise their phone display information, targeting Chinese immigrant communities. This resulted in more than 350 victims across 27 US States and financial losses averaging $164,000 per victim for a total of $40 million. And for 5 years, this scam just kept going. As these scams evolve, groups now face increasingly sophisticated AI-assisted calls, where scammers use technology to convincingly mimic loved ones' voices, further exploiting vulnerabilities, particularly among older adults—many of whom live on fixed incomes or live with economic insecurity.

While social movements have fought to promote economic equity, cybercriminals undermine these efforts by exacerbating financial vulnerabilities. From the 1960's La Causa movement advocating for migrant worker rights to the Poor People's Campaign mobilizing across racial lines, activists have worked to dismantle systemic barriers, end poverty, and push for fair wages. Current attacks on financial systems, however, often target the very groups these movements aim to empower—perpetuating the disparities that advocates have fought against. Digital scams and fraud incidents disproportionately impact those least equipped to recover—including natural disaster victims, people with disabilities, older adults, young adults, military veterans, immigrant communities, and lower-income families. By stealing essential resources, cybercriminals compound hardships for those already struggling to make ends meet or those experiencing some of the worst hardships of their lives—pushing groups deeper into the margins.

Education Access

Education is another area where cybercrime has soared. One of the worst hacks of 2023 exploited a flaw in a file transfer software called MOVEit that multiple government entities, nonprofits, and other organizations use to manage data across systems. This includes the National Student Clearinghouse, which serves 3,600 colleges, representing 97 percent of college students in the US to provide verification information to academic institutions, student loan providers, and employers.

Attacks on educational systems are devastating at all levels. A top target for ransomware attacks last year was K–12 schools. While the complete data is not available yet, by August 2023 ransomware attacks (where hackers lock an organization's data and demand payment for its release) hit at least 48 US school districts—three more than in all of 2022. Schools already have limited resources, and cybersecurity can be expensive, so many have few defenses against sophisticated cyberattacks.

The data compromised in attacks against educational institutions includes identifying information and deeply sensitive student records, such as incidents of sexual abuse, mental health records, and reports of abusive parents. This information can affect future opportunities, college admissions, employment, and the mental health of students. The impacts are especially magnified for students from marginalized backgrounds, who already face discrimination in academic and employment opportunities. In 1954, the US Supreme Court struck down segregated public schools as unconstitutional in *Brown* v. *Board of Education* to address disparities based on race, but today's threats to equitable and accessible education are being jeopardized through digital attacks.

Democratic Participation

Another foundational pillar of our civil rights is also under attack: democracy itself. Since 2016, foreign state actors and state-linked criminals have increasingly used sophisticated cyber operations to suppress minority democratic participation worldwide. The early warnings for the 2024 global elections are clear: Influence and disinformation threats will likely escalate—now enabled by AI-powered cyber operations. Unlike humans, AI systems have few limitations—they can spread disinformation and divisive content to a vast, multilingual, global audience across countless mediums, simultaneously and without rest. Worse, they can do so in an individualized, highly targeted manner.

The undermining of democracy is also more insidious, less about pushing communities toward a specific candidate than sowing distrust in the system itself—which leads fewer people to vote and otherwise suppresses civic participation. The concentration of these attacks on racial and ethnic minority groups means communities of color, who historically have not been in positions of power, will remain marginalized and disenfranchised. Consider a 2022 cyberattack on Mississippi's election information website on that year's Election Day—a significant event in a State without modern early voting options. The 2022 elections included crucial midterm elections that decided congressional representation, and Mississippi has the second-highest Black population (39.2 percent) in the US, behind only the District of Columbia—a jurisdiction without voting rights in Congress. The disruption also extended to State judicial elections, where most judges are elected in a single day, due to a lack of judicial primaries. In Mississippi, 11 percent of adults and 16 percent—of Black voters could not cast a ballot because of past felony convictions. With the compounded challenges in Mississippi—no early voting, no judicial primaries, and the high rate of disenfranchisement—coupled with the opportunity of a pivotal Black voting bloc, access to voting information is imperative for those who can vote.

Weaponizing cyber operations for any form of voter suppression leaves marginalized groups further aggrieved and isolated. Worse, it takes away our only ability to address systemic inequities in wealth, health, and education: democratic participation.

These compounding problems require a new perspective on cyberattacks that looks beyond lost dollars, breached files, or doomsday debates over generative AI tools like ChatGPT or artificial general intelligence. Marginalized communities are suffering now and civil rights advocates cannot take on these burdens alone. To quote civil rights icon Fannie Lou Hamer, "The only thing we can do is work together." Cybersecurity analysts, developers, journalists, researchers, and policymakers must incorporate civil rights into our work by building inclusive defenses, understanding demographic trends in cyber attacks, deterring misuse of AI, and utilizing diverse teams.

Cyber operations are being used to attack the foundation of civil rights, democracy, and dignity around the world, and that is a problem that affects everyone.

Nicole Tisdale is an attorney and founder of Advocacy Blueprints, a firm focused on national security and cyber policy consulting, and advocacy training. Formerly a director at the White House National Security Council and US Congress Homeland Security Committee, Nicole has been an influential voice in global policy dialogs, having participated in 35 international delegations across 22 countries addressing key economic, security, human rights, and intelligence issues.

Ms. CLARKE. Thank you, Mr. Chairman. This article written by Nicole Tisdale, a former staffer of this committee and the National Security Council, provides valuable context on the societal impacts of cyber threats, the need for inclusive cybersecurity strategies.

Developers and deployers of artificial intelligence, whether in the realm of securing the homeland or providing a service to consumers must be thoughtful and intentional in the creation and rollout of this technology.

Similarly, we as policy makers must be deliberate and meticulous in our choices as we work toward major legislative efforts such as creating a framework for the use of AI in securing the homeland as well as in crafting a comprehensive data privacy standard, which remains foundational to our work on AI and the range of other issues.

We must all take care to ensure that civil rights and the principles of our democracy are baked into this emerging technology because once it gets out there will be no putting the genie back in the bottle.

Mr. Sikorski, you have encouraged the Government to consider different standards for different use cases recognizing that certain uses of AI may not pose the same civil liberties concerns as others. Can you elaborate on why you think such differentiation is important and how you think the Federal Government should identify which uses of AI should trigger heightened security while keeping American civil rights top of mind?

Mr. SIKORSKI. That's an excellent question, Congresswoman. I think about, you know, whenever you're applying security to something people see it as an inconvenience and they don't want to do it.

Especially when it comes to innovation as well, people are moving very fast with this technology and we need to think about security as we do it rather than just rushing to get it out there. Because like you said, it's unstoppable once it's out, right, the genie is out of the bottle.

So I think that when I look at cybersecurity specifically and the defense challenges we have, we spoke earlier about the amount of threats and the amount of attacks going up over time, and that our adversaries we also touched upon are leveraging AI and trying to figure out how they could produce more attacks leveraging AI.

So it's very important, I think, to keep innovating very quickly on the security side and focus on, well, that data is the ones and the zeros, the malware, the what's happening on a system, what is vulnerable, and using that as the inputs to make the decisions.

I think when it comes to things like you mentioned, policing, you could go to employment, credit, education, college application, wherever this ends up going it's important to really take a look at those, you know, high-risk cases and take an approach to regulation that has a purpose and why you're doing it. Because in those impacts it's really impacting people's lives in a way that maybe with cybersecurity it's like we're helping people's lives by preventing them getting attacked.

Ms. CLARKE. Very well, thank you.

Mr. Laperruque, do you agree that we should have different standards for different use cases and what use cases do you believe pose the greatest civil rights and privacy risk? Other witnesses are also welcome to chime in.

Mr. LAPERRUQUE. It's there are certainly some types of oversight that should be universal. You know, a lot of the principles I'd mentioned for ensuring accurate results and efficacy you'd want to apply across the board.

But at the same time there are certain forms of AI that do create heightened risk to individual rights and liberties that we do need to have heightened standards and safeguards for. Any type of AI, for example, that might be used to help make a designation that an individual should be the target of an investigation, subject to surveillance, or arrested, that's, you know, an obvious example where there's severe rights impacting ramifications to a use of AI that weren't heightened scrutiny and a number of extra safeguards you would probably want to have in place to make sure that uses are efficacious and that you are not having problems such as the biases that you've mentioned.

Mr. BRECHEEN. The gentlelady yields.

With that, I want to thank the witnesses for your valuable testimony before this committee today. We would ask the witnesses to respond to any additional questions in writing.

Pursuant to committee rule VII(D), the hearing record will be open for 10 days. Without objection, this committee now stands adjourned.

[Whereupon, at 12:53 p.m., the committee was adjourned.]

APPENDIX I

QUESTIONS FROM CHAIRMAN MARK E. GREEN FOR TROY DEMMER

Question 1. Please describe at the unclassified level the nation-state activity Gecko Robotics has observed while scanning critical infrastructure for vulnerabilities.

Answer. Gecko has observed malicious activity from regions of interest for our commercial offering; however, in the field, we have not noticed any activity from foreign nation-states. For U.S. Government assets, all inspections are done on U.S. Government facilities with their own security measures. For commercial inspections, we are not qualified to attribute any interactions as belonging to or related to foreign nation-state actors. As part of our on-going maintenance and protection of our critical digital infrastructure, Gecko Robotics logs internet protocol (IP) location and volume. Because our controlled Government work is air-gapped, we have not observed any malicious activity with regard to Government data. We welcome further discussion of this topic in an appropriate venue.

Question 2. How should policy makers think about AI "risks"—which ones should we worry about today, and which are perceived risks? What steps can AI developers take today to ensure that we can mitigate "existential risks" if we ever reach that AI capability?

Answer. Policy makers should prioritize the risk of bad data inputs to the development, training, and testing of AI. Bad data inputs are not a perceived risk; they represent a real and current risk to many deployed and in-development AI algorithms. The outputs of AI trained on bad data inputs are used by Americans every day for decision making. Bad inputs produce bad outputs, and while some of these bad outputs are comical, others may be dangerous.[1]

AI models are only as good as the inputs they are trained on. Trustworthy AI requires trustworthy data inputs, and so policy makers should create policies that mitigate the existential risk of bad data by ensuring all data used to develop, train, and test AI is accurate, auditable, and interrogatable—with clear traceability from the time, place, and method of data creation to the point of its use in AI development.

Building a data foundation has proven to be one of the biggest challenges to effective AI development. Without robust, interrogatable/audible, accurate, and verifiable/trustworthy data, AI models present an outsized risk to Americans by delivering suboptimal or incorrect results—with potentially hazardous consequences. We encourage policy makers to create robust data quality frameworks and hold AI companies accountable for data transparency.

Question 3. What cybersecurity practices does Gecko Robotics implement to ensure IP protected and to proactive mitigation of harms against your company?

How does Gecko Robotics secure its digital twins to ensure they do not inform the activities of potential cyber attackers, especially nation-state actors?

Answer. Gecko Robotics maintains strict security requirements for its on-premises data collection environment as well as its Cloud environment for data processing and application delivery. These protections help support the security of customer data and information, including data and information provided by the DoD. To ensure comprehensive security coverage, we leverage trusted partners. These partners include Managed Security Service Partners (MSSP), Platform as a Service (PaaS) providers for compliant infrastructure, and independent security consultants for offensive security expertise and annual penetration testing.

[1] A recent *Washington Post* article reported that Google scaled back its AI after outputs told readers to put glue on pizza and informed them Barack Obama was Muslim. The bad outputs were sourced from bad inputs (i.e., social media posts that contained false information): *https://www.washingtonpost.com/technology/2024/05/30/google-halt-ai-search/*.

Gecko Robotics secures its cloud-hosting environment in a number of ways designed to keep pace with the ever-evolving threat landscape; these include adopting practices that align with frameworks approved by the DoD, including NIST 800–171 and 800–172 and, where applicable, partnering with third-party PaaS providers with authority to operate.

Question 4. What can the U.S. Government do to improve its partnership with industry? Conversely, how can industry best serve the U.S. Government?

Answer. Regarding the effective and ethical deployment of AI, the U.S. Government can improve its partnership with industry by providing industry with secure access to current, high-fidelity, high-volume data. Using this data, industry can serve the Government with AI that improves cybersecurity, national security, physical infrastructure, human health, etc.

In order to generate this data for physical infrastructure—one of the cornerstones of not just national security but the American way of life—the U.S. Government must invest in technologies for accurate data collection on critical assets. This means putting R&D funding toward the development of hardware technologies (such as robots, drones, sensors, etc.) that can collect high-fidelity, high-volume data. It also means contracting with companies that can leverage these hardware technologies on a regular basis to ensure accurate, updated data is available for evolving AI development for U.S. Government efforts and initiatives.

Specific actions we recommend the U.S. Government take include:

- *Providing adequate testing environments for AI-enabling hardware development.*—Under Executive Order 14110, DHS is an important partner in "developing and helping to ensure the availability of testing environments, such as testbeds, to support the development of safe, secure, and trustworthy AI technologies . . . ". DHS can provide qualified companies with access to adequate testing environments to develop AI for physical infrastructure.
- *Design funding programs for the realities of hardware development.*—Unlike software, which can be rapidly prototyped and scaled, hardware development often demands more engineering staff and longer testing periods. DHS can develop programs that recognize and account for the unique requirements of hardware development. For example, programs like DHS's Silicon Valley Innovation Program (SVIP) provide huge opportunities to develop hardware systems to develop hardware systems that can drive the development of safe and reliable AI for national security. However, the current headcount (<200 FTE) and funding (<$1 million in Federal contracts) requirements limit the ability of hardware-focused start-ups to participate.
- *Opt into Majority VC ownership authority for DHS SBIR program.*—DHS's Small Business Innovation Research (SBIR) program has to date not opted into the "Majority VC ownership" authority (as specified in 15 U.S.C 638(dd)). This means that many VC-backed companies developing AI or AI-enablement technologies are ineligible to apply to this competitive program. DHS should consider opting into this authority.

Question 5. As a start-up company, do you face—or do you anticipate facing—AI regulatory compliance challenges to complete your work? How can, or is, AI helping you to fulfill these requirements?

Answer. Because of the scale and type of AI development at Gecko Robotics, we do not anticipate facing AI regulatory compliance challenges.

Question 6. How do you think the evolving AI regulatory landscape will influence the decisions of entrepreneurs like yourself to take the leap to start a company?

Answer. Like all entrepreneurs in the technology space, we are eager to leverage AI for the benefit of our customers and our business; however, the evolving AI regulatory landscape—and, at times, even the evolving definition of AI—can make advanced AI utilization risky, especially for a small business like ours.

Regulatory uncertainty requires all companies interested in pursuing AI to continuously update their understanding of compliance requirements and potential restrictions. Over the last several years, regulatory bodies have developed, updated, and evolved their understanding of AI and its risks. In response, they've released new regulations and guidelines to protect consumer privacy, prevent misuse, and ensure ethical standards are upheld. These new regulations and guidelines have been important for supporting responsible AI development and deployment. However, the shifting environment has generated several challenges for small businesses:

- *Changing guidance and regulation creates a sense of unpredictability, making it challenging to plan long-term AI development strategies.*—For a small business, this requires continually updating our software development roadmap, diverting substantial time and resources away from innovation and growth.

- *Compliance with evolving regulations can require substantial investment in legal, technical, and administrative resources.*—For a small company, these additional costs could be prohibitive, potentially putting them at a disadvantage compared to larger, more established firms that have more robust compliance infrastructures.
- *Influencing evolving regulations is a time-consuming and sometimes cost-prohibitive process for some small businesses.*—To ensure that the interests of small businesses are taken into account, Gecko Robotics invests substantial time and resources into staying informed about regulatory trends, participating in industry groups, and conducting outreach to Congress to support policy that is beneficial for all American companies and consumers.

While these challenges are significant, the AI regulatory landscape also presents opportunities for small businesses. Regulation, when done effectively, can level the playing field by setting fair industry standards, potentially curbing unfair advantages and promoting healthy competition.

Question 7. From your experience working in the field, what types of AI research and development (R&D) projects should the Government be involved in, and what is the private sector best suited to solve? Are there any areas where your company lacks understanding in AI?

Answer. The Government should be involved in AI R&D that affect American companies and citizens, though to varying degrees. The Government may choose to be directly involved in the AI R&D that affect Government operations, regulation, and national security. The Government may choose to be involved in other types of AI R&D indirectly—for example, through the development of regulatory and compliance frameworks and the enforcement of policy.

Gecko develops AI models to assist companies and governments in making decisions regarding their physical infrastructure. We currently lack deep understanding in the types of AI capabilities that the Government is seeking to achieve for physical national security infrastructure, including bridges, tunnels, power plants, etc. We would be interested in partnering with the Government to bring AI R&D to these key assets.

Question 8. The United States currently does not have a comprehensive data privacy law. Instead, it has a "patchwork" approach that includes many different laws across States.

Have disparate data privacy laws posed—or do you anticipate that they will pose, as AI models quickly evolve—challenges with safe and secure AI development and deployment?

Answer. Because most data privacy laws pertain to data collected on people (for example, personally identifiable information [PII] and protected health information [PHI]), most data privacy laws do not apply to Gecko Robotics, since our AI uses data collected from physical infrastructure. However, we recognize how a patchwork approach to data privacy may create a challenging compliance landscape for companies that work in this space.

Question 9. How does Gecko Robotics foster collaboration and compatibility among AI systems used by various national security agencies to ensure seamless communication, data sharing, and coordinated responses to emerging threats?

Answer. Gecko Robotics is not currently connected to AI systems used by national security agencies.

Questions From Chairman Mark E. Green for Michael Sikorski

Question 1. How should policy makers think about AI "risks"—which ones should we worry about today, and which are perceived risks?

Answer. We believe policy makers should employ a risk-based approach when considering AI guardrails that takes into account differences in the use cases, the data processed in those use cases, and the potential resulting impacts on individuals. There are fundamental differences in risk between AI systems that, for example, leverage consumer data to make or facilitate consequential decisions with legal, material, or similar impact for individuals—as compared with those that leverage security data to ensure the robustness and resilience of networks.

When AI is used to make consequential decisions about credit, housing, employment, health care, or insurance, for example, those decisions have a significant impact on individuals. By contrast, when AI is deployed to enable cybersecurity tools to stitch together security data much more quickly and effectively than before, the result is that society as a whole is better protected and all individuals benefit.

We urge policy makers to carefully consider the varied nature of AI use cases to ensure that any new guardrails do not unintentionally inhibit the continued and expanded use of AI-powered tools for cyber defense.

Question 2. What is your relationship with the Cybersecurity and Infrastructure Security Agency (CISA) on AI activities, and how do you think this relationship is helped or hindered by CISA's AI framework?

Answer. We maintain a close relationship with CISA on a range of activities and are proud to be a founding alliance member of CISA's JCDC. We recently participated in a JCDC tabletop exercise that is supporting development of an AI Security Incident Collaboration Playbook spearheaded by JCDC. AI, a dedicated planning effort within JCDC focused on building an operational community of AI providers, AI security vendors, and other critical infrastructure owners/operators to address risks, threats, vulnerabilities, and mitigations concerning AI-enabled systems in national critical infrastructure.

We found this tabletop exercise to be valuable and look forward to continuing to engage in these forums.

Question 3. We have yet to see whether AI defenders or attackers will benefit the most from generative AI for cybersecurity. However, several U.S. Government officials believe that defenders currently maintain the advantage.

From your perspective, who stands to benefit the most from generative AI—attackers or defenders? Please describe how you've seen both attackers and defenders use generative AI.

Answer. As my written testimony highlighted, AI is of course being leveraged by both attackers and defenders. Adversaries are always evolving, with or without AI, and as a cybersecurity community we can never get complacent.

With that said, our company is extremely encouraged by the transformative benefits AI is already showing for cyber defense. Because of AI, every day Palo Alto Networks is able to detect 2.3 million never-before-seen attacks. AI-powered SOCs have also reduced our customers' mean time to respond from 2–3 days to under 2 hours.

It's evidence like this which underscores why Palo Alto Networks is doubling down on its use of AI for cyber defense. All of our platforms are now infused with Precision AI, which combines the best of machine learning, deep learning, and the natural language processing capabilities of generative AI to help defenders stay a step ahead of attackers.

Question 4. There are many conversations globally about establishing accepted practices for the development, deployment, and use of artificial intelligence. However, ambitious adversaries, such as China, Russia, and Iran, appear more concerned with technological advancement than ethical use.

What are some practical steps companies can take to ensure they harness AI responsibly without creating more vulnerabilities caused by cautious building?

Answer. AI app proliferation is changing how enterprises operate and necessitates an evolved security approach. We like to think of this approach as Securing AI By Design. This approach requires the ability to:

- Secure every step of the AI app development life cycle and supply chain.
- Protect AI applications, models, and data from threats in runtime.
- Oversee employee AI usage to ensure compliance with internal policies.

These principles are aligned with—and based on—the security concepts already included in the NIST AI Risk Management Framework (RMF). Palo Alto Networks would welcome the opportunity to continue engaging with Members of the committee and staff about how we can promote these principles for ecosystem-wide benefit.

Question 5. How challenging is it to create safeguards for generative AI models? How should we determine if a model is "good enough" for national security use cases to ensure we do not slow down innovation?

Answer. While there is no silver bullet, we would encourage all AI models in national security use cases to employ AI Security Posture Management (AI–SPM). AI–SPM is a vital component in digital ecosystems where AI plays a pivotal role. Both the adoption of AI and AI systems themselves present unique vulnerabilities and attack surfaces that demand mechanisms for the visibility, assessment, and mitigation of risks associated with AI components within technology ecosystems.

AI–SPM entails securing AI models, algorithms, and systems and addresses the unique challenges posed by AI technologies, such as adversarial attacks, data poisoning, model stealing, bias, and unauthorized access. It encompasses secure model training, privacy-preserving AI techniques, defense against attacks, and explainability. By implementing AI–SPM, organizations can proactively protect their AI systems from threats, minimize data exposure, and maintain the trustworthiness of their AI applications.

Question 6. From your experience working in the field, what types of AI research and development (R&D) projects should the Government be involved in, and what is the private sector best suited to solve? Are there any areas where your company lacks understanding in AI?

Answer. As a company, we support public investment in AI research to help ensure that the United States maintains a leadership role in AI innovation. To that end, Palo Alto Networks supports opportunities and resources for companies of all sizes to partner with Federal research centers focused on AI R&D, including the National AI Research Resource (NAIRR). The Federal Government should continue incentivizing R&D activity and promote public-private partnerships and industry best practices.

Question 7. How does Palo Alto foster collaboration and compatibility among AI systems used by various national security agencies to ensure seamless communication, data sharing, and coordinated responses to emerging threats?

Answer. AI-powered tools can actually facilitate data sharing because they can normalize and stitch together security data to make it more actionable. For example, the AI-powered SOC on our company's own networks ingests 59 billion events a day but is able to analyze and triage that diverse universe of security data down to just 75 alerts that require further analysis. Staying ahead of emerging threats will benefit from deployment of similar capabilities so that national security personnel can nimbly separate the signal from the noise.

QUESTIONS FROM CHAIRMAN MARK E. GREEN FOR AJAY AMLANI

Question 1. Please describe why biometrics matter for the AI industry. How does iProov think about data collection, management, and retention?

Answer. At iProov, we are committed to utilizing AI and deep learning to revolutionize the identity verification industry. Our state-of-the-art algorithms, developed by our team of AI experts, harness the potential of deep learning techniques to analyze and interpret inherent human characteristics with market-leading precision.

By employing advanced methodologies such as convolutional neural networks (CNNs), we have achieved remarkable accuracy in image recognition tasks, enabling us to deliver robust biometric authentication and identification systems. Because deepfakes are now indistinguishable to the human eye, AI-powered solutions are now vital in mitigating the risk they pose to remote identity verification.

In a rigorous process conducted by Ingenium Biometrics, a FIDO face verification accredited lab, which consisted of no less than 10,000 tests, iProov's Dynamic Liveness achieved a flawless success record with no attacks passing the system. These results set a new benchmark for accuracy and reliability.

Our AI team of experts' key responsibility is continuously iterating and enhancing our system to meet the demands of security, performance, and inclusion, adhering to W3C WCAG 2.2 AA and ADA Section 508. This requires a deep understanding of the latest advancements in AI and deep learning and the ability to translate business requirements into technology design.

We recognize that the ethical use of AI is of paramount importance. Our team ensures that our AI systems are developed and deployed transparently, with clear accountability, and aligned with our values. These values guide our decisions and actions, ensuring we deliver secure, reliable, sustainable identity verification solutions.

The protection of biometric data is of utmost importance, especially in the context of AI and digital identity verification. As a leading provider of biometric verification services, we have implemented comprehensive measures to ensure the security and privacy of the data we collect, manage, and retain.

iProov has a thorough Security and Incident Management team, that includes physical access, and reviewed on an annual basis as part of its obligations to ISO27001.

iProov regularly conducts tabletop planning security exercises to test the readiness and resilience of a particular department in the event of a security incident.

iProov is regularly externally audited against key security certifications, which include our security incident management procedures. The following table details our most recent audit certificates and reports:

- ISO 27001 Certificate
- ISO 27001 Statement of Applicability
- SOC2 Report
- CSA Star Level 2 Report
- CSA Star QAIC Mapping.

The principles of transparency, minimization, consent, and necessity guide our data practices. We collect biometric data solely to provide secure verification services to our clients and their users. Our platform employs advanced cryptographic controls, to safeguard the biometric data entrusted to us. We adhere to stringent industry best practices and security standards in our key management processes to maintain the integrity and confidentiality of the data we handle.

Regarding data management, iProov takes a proactive stance by following a rigorous Information Security Management System Software Development Lifecycle (ISMS SDLC). This comprehensive framework encompasses all aspects of our software development process, from handling information security and ensuring source code quality to identifying and addressing security vulnerabilities. We leverage security tools provided by leading cloud platforms to fortify our defenses against potential threats. Our ISMS SDLC ensures that data security is embedded at every stage of our software development life cycle, from conception to deployment.

Data retention is another critical aspect of our privacy-centric approach. At iProov, we strictly limit the retention period of all data in accordance with the General Data Protection Regulation (GDPR). We understand that personal data, particularly biometric information, is highly sensitive and must be handled with the utmost care. As such, we have clearly-defined retention times for both personal data and special category personal data, which are outlined in our contracts with clients. By adhering to these retention policies, we minimize the risk of data breaches and ensure that personal information is not retained any longer than necessary.

In summary, iProov's commitment to leveraging the power of AI and deep learning, combined with the expertise of our specialist AI team, positions us at the forefront of the identity verification industry. We are unwavering in our commitment to maintaining the biometric industry's highest data privacy and security standards. Our robust data collection, management, and retention practices are designed to protect the sensitive information of our clients and their users while enabling the secure and efficient deployment of AI-powered identity verification solutions.

We will continue to invest in technologies and adhere to evolving industry best practices to deliver authentication and identification systems that are secure, reliable, and seamlessly integrated into our users' lives. We remain dedicated to harnessing AI's potential as we grow and evolve.

Question 2. How does iProov monitor and address identified vulnerabilities in the company's AI and networks?

Answer. At iProov, we have implemented a comprehensive approach to monitor and address vulnerabilities in our AI systems and networks through our dedicated iProov Security Operations Center (iSOC). The iSOC integrates advanced technology, standardized processes, and highly-skilled security experts to proactively detect, respond to, and mitigate potential threats to our biometric security platform. Fully audited across a range of attack scenarios, our solution is tested to National Security Standards by the U.K. Home Office, the Singapore Government, the Australian Government, and the U.S. Department of Homeland Security.

In addition, iProov-powered solutions conform to EN 319–401, certified by independent auditors, including TÜV Informationstechnik GmbH and Ernst & Young for conformance to eIDAS Clause 24 1(d).

Our iSOC employs sophisticated anomaly detection algorithms that continuously analyze production traffic from various devices, platforms, and geographies to identify suspicious activities or potential vulnerabilities. These algorithms utilize technologies such as artificial intelligence, machine learning, and computer vision to enhance the accuracy and efficiency of threat detection.

The iSOC follows a rigorous process that includes regular security audits and assessments to identify vulnerabilities and areas for improvement. This process is further strengthened by close collaboration with our Threat Intelligence and Red Teams, ensuring that the latest threat intelligence is incorporated into our monitoring and detection mechanisms.

The Threat Intelligence team proactively monitors external threat actor behavior, analyzes trends in attack patterns and tactics, and conducts threat hunting to identify emerging threats. They collaborate with industry partners and law enforcement agencies to share intelligence and coordinate responses to novel attack methods.

Our Red Team, composed of experienced security professionals, conducts sophisticated adversary simulation activities to test the resilience of iProov's biometric security solutions thoroughly. They assess a wide range of potential attacks, including presentation attacks, deepfake, synthetic identities, face swap and injection attacks, as well as traditional penetration testing, to identify any vulnerabilities in our systems.

Based on the Red Team's findings, our Science Team, consisting of experts in AI, MLOps Engineering, and Synthetic 3D Data Research, takes appropriate action. If the Red Team determines that a new attack tool or method could expose a vulnerability, the Science Team immediately develops and deploys new security tools and technologies to counter the threat. The turnaround time from alert to deployment typically ranges from 24 to 72 hours, depending on the severity and nature of the vulnerability.

This collaborative feedback loop, involving the iSOC analysts, Threat Intelligence team, Red Team, and Science Team, ensures that iProov's Biometrics-as-a-Service offering remains at the forefront of biometric security. By continuously monitoring, identifying, and addressing potential or future vulnerabilities in our AI systems and networks, we maintain the highest level of security and performance for our clients and their users.

This commitment to on-going security enhancement allows organizations to confidently leverage the benefits of our biometric authentication solutions while minimizing the risk of fraud and cyber crime.

Question 3. Please describe your relationship with the Cybersecurity and Infrastructure Security Agency (CISA) on AI activities. Does iProov align its technologies with CISA's Secure by Design principles for AI?

Answer. At present we have no relationship with CISA, but we are currently identifying opportunities to support their priority objectives as they look beyond their 2023–2025 Strategic Plan. As we provide security against deepfake (or digital injection) attacks to operators of critical infrastructure, such as border control and financial and government services, in major markets around the world, including those of key U.S. allies (UK and Australia), as well as in the United States, we are well-positioned to contribute. In addition to sharing with CISA our experience of identifying new and novel AI-generated threats, we can provide support on how identity verification solutions can be most effectively designed and deployed to secure the critical national infrastructure at the heart of the CISA focus.

iProov is a supporter of the goals underpinning the CISA Secure by Design framework. Our solutions are designed to help our customers and partners to deliver against these security goals. By way of example, the focus on enhanced use of multi-factor authentication (MFA) is at the very heart of what iProov delivers. It is our view that when properly deployed MFA has served to improve the security of users and organizations. We argue that the principles behind MFA remain robust (something you know, something you have, something you are), the application must be responsive to the needs of the use case and, in particular, the risk faced in that use case. Passwords or even one-time passcodes may be appropriate for low-risk use cases, but where services are liable to sophisticated cyber attacks, including AI-generated deepfakes, then the MFA solution must adapt to incorporate biometric inherence (something you are) as standard. Moreover, biometric authentication must incorporate Liveness detection as standard such that a malicious actor cannot easily bypass the security using some form of synthetic image. With regards to the pledge to reduce vulnerabilities, our active Threat Intelligence capabilities enable us to identify new and novel threats to our customers and partners, such that we are able to design mitigations to those vulnerabilities at pace and deploy them rapidly across our network.

Although we are not ourselves a signatory to the CISA Pledge, our relationship with the DHS places a requirement on us to adhere to the goals where appropriate. This shared commitment to meeting the highest standards in cyber resilience is evidenced by the accreditations and certifications we hold and against which we are regularly tested. In addition to structured testing by NIST, iBeta, and FIDO, where we are the only certified face verification solution provider, we are also subject to independent red team penetration testing by expert groups including Outflank and AIS. We are also tested regularly for resilience by our partners and customers, including the Department of Homeland Security and the Singapore Government's GovTech program.

Question 4. How can a biometric vendor like iProov help to combat deepfakes? As deepfakes proliferate and become more believable due to advances in AI, what should be the relationship between organizations that use AI in the public and private sectors, including social media companies, to detect mis-, dis-, and mal-information?

Answer. With the volume of AI-generated content increasing exponentially, it is likely to be the case that a mix of policy and technology solutions will be required to tackle disinformation, with the exact mix determined by the use case. For so long as content accreditation systems can be quickly overwhelmed (or indeed gamed by AI, such that false accreditations will quickly materialize), expectations on the likely success of such systems should be carefully managed. That does not mean that there should not be experimentation with such approaches. In cases where it is important to have traceability of content back to its source, and for the end-user to have confidence in the integrity of the source of the content then it is likely that an automated biometric identity verification approach, based on liveness and one-time biometrics, would be most appropriate. Moreover, tying social media to ID would lead to an increase in personal accountability for content and communications. Improving levels of accountability would change the behaviors of many on social media platforms. With specific regards to nation-state actors using bots and digital manipulation techniques to try and influence the outcome of elections and the political process, we believe that only ID verification of account holders can solve this—there is no other way.

We do not underestimate the complexity of addressing the challenge of delivering such an outcome in practice, given the scale and regulatory obstacles. It may be advisable to identify and prioritize those context(s) within which false images and content may be most damaging and where the identification of false images is most technically and economically feasible.

With regards to determining the validity of a media presenter, as opposed to a piece of audio or text, the crucial first step is to be aware that deepfakes and synthetic digital injection attacks (whereby synthetic media is injected into the data stream, bypassing trusted device authentication) are both real and increasingly common. U.S. Government agencies have shown leadership in their awareness of these threats.[1] The availability of generative AI means that the technical know-how barrier is evaporating, allowing less tech-savvy attackers access to on-line tools to create false images, including 3D face swaps, audio, and text, which have also become more sophisticated to the point where they are impossible to discriminate with the naked eye (near-human fidelity) or ear. Publicity and media coverage further serves to drive curiosity and interest in testing the capabilities of AI both by malicious actors and by the moral majority—those who would never set out intentionally to act unlawfully.

The second step is detection. Once these attack tools are successful across certain platforms, they are then sold on to organized groups. With reduced accessibility barriers, increased tool sophistication, and a perception that tools to create deepfakes can be "fun" applications, the sheer volume of faked images and content can prove overwhelming for those trying to identify and isolate the work of malicious actors. It's alarmingly apparent that these threats are challenging even for state-of-the-art machine-learning computer vision systems. We now need to include other complementary, multimodal approaches as imagery is becoming increasingly veridical—we can no longer solely rely on the trained human eye or even computer vision. Furthermore, privacy features on desktop and mobile devices are making it challenging to verify device authenticity, allowing attackers to conceal their identity and method of attack. Detection of a presentation attack detection (PAD), whereby a mask, photo, or video playing on a screen is presented to the camera in an attempt to create a faked image, is relatively straightforward and well-understood. Detection of injection-based attack vectors is more challenging, and more sophisticated tools are required, such as looking at the metadata or other information that comes from the device or detecting that the imagery has been synthesized or modified in some way. However, this is not straightforward. What's more, unlike PAD, there are no globally-accepted standards pertaining to digital injection attack detection. This has given malicious actors an advantage in the biometric arms race as defenses blindly fail to keep up with novel attacks.

Question 5. The AI Executive Order permits the use of the Defense Production Act to collect certain information for potential dual-use foundation models, including model weights and the physical and cybersecurity practices that protect model weights.

Do you have concerns about the concentration of sensitive or proprietary information associated with your AI models? How do you handle sensitive information at your company today?

Answer. As a leading provider of biometric authentication services, we have implemented robust measures to ensure the security and confidentiality of the data we process, including the data used to train and optimize our AI models.

Under the E.U. and U.K. GDPR, we act as a processor for our clients, who are the controllers of personal data. We adhere to the purposes and retention periods authorized by our clients in their written contracts with iProov. For facial imagery provided by end-users (data subjects), the typical retention period is 30 days from enrollment or deletion of the end-user in the case of an on-going authentication service.

We have implemented a firewall to ensure that any personal data from end-users, including facial imagery and the resulting biometric template, is pseudonymized and cannot be directly associated with an identifiable person by iProov. This pseudonymization helps protect the privacy and security of the sensitive information associated with our AI models.

[1] Public-Private Analysis Exchange Program, "Increasing Threat of Deepfake Identities," *https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf,* 2021.

Our 30-day data retention policy for pseudonymized imagery and related data is carefully designed to balance the rights of data subjects with their security expectations. This retention period allows us to identify sophisticated attacks that may occur over an extended period, typically ranging from 30 to 120 days, based on threat risk factors. By retaining data for 30 days, we can effectively detect and counter complex attack patterns while respecting data subjects' privacy rights and reasonable expectations.

During this 30-day period, with the consent of our clients, we process facial imagery using research methodologies intended to optimize performance according to internationally approved standards (ISO/IEC 30107–3:2017 or successor standards). This processing helps minimize bias in our AI models, ensuring that factors such as ethnicity, gender, and age do not adversely affect the performance of our biometric authentication services.

In summary, while we acknowledge the potential concerns surrounding the concentration of sensitive information associated with AI models, iProov has implemented stringent measures to protect this information. Our data retention policy, pseudonymized data, and adherence to international standards and best practices for bias mitigation allow us to effectively balance the security needs of our clients and end-users with data subjects' privacy rights and expectations. We remain committed to handling sensitive information with the utmost care and diligence to maintain the trust and confidence of our clients and their end-users.

Question 6a. In April, DHS announced the AI Safety and Security Board (AISSB) to fulfill a requirement under the AI Executive Order, which was issued in October 2023. The AISSB includes the biggest tech companies, such as OpenAI and Google, as well as civil rights organizations and sector-specific companies, such as Delta Airlines.

Is it possible to get a diverse group of stakeholders to discuss "AI", which does not have an agreed upon definition, and "AI risks" in the same way? If not, how should the AISSB tackle these issues?

Question 6b. What safety and/or security issues would you have the AISSB focus on?

Answer. That there are differences in interpretations and understanding of AI and AI risks can be healthy at this stage in the development both of the industry and of the supporting policy framework. For example, although the term AI is used commonly, formal definitions are likely to be time-limited and dependent upon context. Moreover, there is a slide scale of technologies covering the spectrum of machine learning through to general purpose AI tools, and indeed many technologies could potentially fit within multiple definitional constraints depending on how it is used. Until there are settled definitions which are built into a stable legal framework there is more to be gained by promoting a diversity of viewpoint, rather than striving for a fixed and narrow definition. Such diversity will stimulate and drive a discussion and debate across parties, promoting cross-learning and potentially triggering yet further innovating thoughts. Through engagement with these diverse opinions and subsequent debates, policy makers, agencies, and regulators will be better informed on the potential opportunities to support innovation as well as to introduce targeted interventions to mitigate likely harms.

As the committee has observed, there are real and present risks associated with malicious use of generative AI tools to create fake identities for the purpose of committing identity fraud, for spreading disinformation, as well as other forms of unlawful and socially disruptive acts. Our request is that the Board be directed to focus primarily on identifying real and present risks, such as those posed by deep fakes, and engage widely to identify routes to industry-led market solutions. Where a market-led solution proves infeasible, the Board should engage with policy makers, share the learnings from such a process, and work collaborative in the development of policy interventions where proven necessary.

Question 7. What cybersecurity practices does iProov implement to ensure its IP is protected and to proactively mitigate harms against the company?

Answer. iProov implements a comprehensive set of cybersecurity practices to protect its intellectual property (IP) and proactively mitigate potential harms against the company.

We adhere to various industry standards and regulations, demonstrating our commitment to robust cybersecurity practices. These include:

- ISO 27001:2013 certification for its Information Security Management System (ISMS)
- Conformance with ISO/IEC 30107–3:2017 for Presentation Attack Detection (PAD) testing
- Conformance with ISO/IEC 19795–1:2006 for biometric verification performance testing

- IRAP (Information Security Registered Assessor Program) audited in Australia, achieving the highest level of Identity Proofing (IPD 3)
- Compliance with European GDPR and UK Data Protection Act 2018
- Conformance with eIDAS (electronic IDentification, Authentication, and trust Services) regulations
- SOC 2 Type II certification
- Conformance with W3C WCAG 2.2 AA, and ADA Section 508 accessibility guidelines
- FIDO Alliance face verification certification.

Secure Infrastructure and Data Center Practices

iProov uses major cloud infrastructure as a service (IaaS) providers with stringent access and entry controls, including barriers, entry logging, airlocks, closed-circuit television, and RFID entry with booked access times, restrictions, and exit times.

iProov's hosted services are specifically built for resilience by the cloud service providers with internal "Availability Zones," each with segregated power, network, HVAC, and backup systems. The centers are not sited on floodplains or in areas where they are susceptible to natural disasters. Each of the 3 main providers gives detailed certification of their facilities via their websites. This includes SOC 2 reports.

All cloud providers have gone through iProov's procurement process, undertaken due diligence checks, and have the required contracts in place. Part of such checks ensures that adequate physical security controls are in place.

Access Control and Management

iProov implements strict access control and management procedures to restrict business data and resource access. This includes:

- Authentication and authorization mechanisms
- Access control rules and rights based on standard user profiles and business requirements
- Segregation of user access requests, authorization, and administration
- Adherence to the principle of least privilege
- Regular review and amendment of user access rights
- Timely removal and modification of access.

iProov has access control and access management procedures in place to restrict who has access to business data and resources. Secure access control principles are employed to ensure that users are who they claim to be and that appropriate levels of access controls are granted. iProov Ltd controls access to information based on business and security requirements.

Access control can broadly fit into the following categories: authentication, authorization, access, management, and audit.

Access control rules and rights to applications are expressed in standard user profiles for each user or group of users and are clearly stated, together with the business requirements met by the controls.

The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

Management of access rights across the network(s) is done by administrators. User access requests, authorization, and administration are segregated. User access requests are subject to formal authorization using the iProov System Access Log, which is subject to periodic review and amendment.

iProov operates under the "least privilege" framework, whereby access is only granted where and when deemed necessary. All users who need to access iProov information have specific, predetermined access rights to that information, operating systems, and applications that conform to and are restricted by the Access Control Policy. Access to the information and application system functions is restricted. User account management includes the timely removal and modification of access.

Users are only provided access to the network and network services they have been specifically authorized to use. User registration, de-registration, and access provisioning are in place. Privileges are allocated only to those users requiring them and are reviewed on a regular basis.

Patent Protection

iProov's technology is protected by over 29 patents, covering various aspects of its facial verification, anti-spoofing, and user experience methods. These patents help safeguard iProov's intellectual property and prevent unauthorized use or replication of its technology.

Continuous Improvement and External Audits

iProov continuously aims to improve its technical security controls through yearly external audits, multiple internal audits, and compliance with various standards such as ISO 27001, IRAP, eIDAS, eID, and SOC–2 Type II. These regular audits and assessments help identify potential vulnerabilities and ensure that iProov's cybersecurity practices remain up-to-date and effective in mitigating risks.

Research and Development

By implementing these comprehensive cybersecurity practices, iProov demonstrates its commitment to protecting its intellectual property and proactively mitigating potential harms against the company. The combination of compliance with industry standards, secure infrastructure, access control measures, patent protection, continuous improvement through audits, and on-going research and development efforts creates a resilient security framework that safeguards iProov's technology and data.

Question 8. Can you describe the new challenges presented by generative AI and how these differ from traditional machine learning?

Answer. Generative AI presents several new challenges that differ from traditional machine learning in the context of remote identity verification and biometric security:

(1) *Realistic synthetic media generation.*—Generative AI, particularly in the form of deepfakes and face swaps, enables the creation of highly realistic synthetic media. Unlike traditional machine learning, which primarily focuses on pattern recognition and classification, generative AI can produce convincing fake images, videos, and audio that closely resemble real individuals.

(2) *Increased accessibility and ease of use.*—Generative AI tools, such as DeepFaceLive, Swapface, and Deepswap, are becoming more accessible to threat actors, with many offering free tiers for experimentation. This wide-spread availability makes it easier for attackers to create sophisticated synthetic media without significant financial investment, unlike traditional machine learning, which often requires specialized knowledge and resources.

(3) *Combination with traditional cyber attack tools.*—Threat actors are combining generative AI-derived synthetic media with traditional cyber attack tools, such as emulators and metadata manipulation, to create new and difficult-to-detect attack vectors. This combination of techniques presents a unique challenge compared to traditional machine learning-based attacks, as it exploits both the visual and technical aspects of biometric verification systems.

(4) *Rapid evolution and adaptability.*—Generative AI techniques are evolving at an alarming pace, with threat actors quickly adopting and adapting new tools and methodologies. This rapid evolution makes it challenging for identity verification systems to keep up with the latest threats, as opposed to traditional machine learning-based attacks, which may be more static and easier to detect and defend against.

(5) *Difficulty in detection.*—Generative AI-based synthetic media, such as deepfakes and face swaps, can be extremely difficult and sometimes impossible for humans to detect consistently. This poses a significant challenge for remote identity verification processes that rely on human operators or less advanced AI techniques, as they may struggle to identify and prevent sophisticated generative AI-based attacks.

To address these challenges, biometric verification systems must utilize multi-layered defense strategies. They must include advanced AI techniques, such as passive challenge-response mechanisms with multi-frame liveness detection, alongside biometric security experts to proactively gather threat intelligence and monitor as well as test the platform regularly to stay ahead of the rapidly-evolving generative AI threat landscape. This requires a more dynamic and adaptive approach compared to traditional machine learning-based security measures.

Question 9. From your experience working in the field, what types of AI research and development (R&D) projects should the Government be involved in, and what is the private sector best suited to solve? Are there any areas where your company lacks understanding in AI?

Answer. In the field of digital identity verification, we do not see a neat separation between the Government and private sectors in terms of the pursuit of research and development opportunities. The power of Government and their agencies to concentrate funding in support of innovation is tried and tested and should be recognized and respected. The work of the Department of Homeland Security to encourage and reward innovation through open competitions and challenges for cybersecurity solutions is largely responsible for the United States continuing to play a global leadership role in the development of robust border security technologies. Agencies should continue to promote innovation through such open competitions, which are particularly important where they are tied to subsequent procurement exercises. The power of the Government and its agencies in the procurement of cyber solutions is also significant for pump-priming private-sector investment. The Government is able to produce at such scale and contract for long-term relationships that private-sector companies feel confident to invest in innovation and engage with new and novel use cases. Similarly, the Government and its agencies play a powerful role through to the testing framework for new technologies. NIST testing for identity solutions is globally respected and every notable solution provider competes vigorously for the top end of NIST tables. This testing in itself is a driver of innovation and competition and the committee should look at how NIST can be further supported as the burden of demand for testing of AI applications increases.

Questions From Chairman Mark E. Green for Jake Laperruque

Question 1. How should policy makers think about AI "risks"—which ones should we worry about today, and which are perceived risks?

Answer. AI poses a wide range of risks, especially in the national security space where stakes are highest for safety and civil liberties alike. Unfortunately, given the pace of innovation and lack of transparency into Government activities in this space, the public does not have a full picture into which types of systems and uses present on-going harms or imminent risk, and which are purely theoretical. Assessing where risks exist and what are the most significant problems to take on is precisely why transparency and oversight measures—such as the AI Oversight Board and annual public reporting described in my testimony—are so crucial.

Overall, use of AI in the national security space presents significant risks to public safety and civil liberties alike. Responsible development and use is key to efficacy. If the Government employs poorly-developed AI systems, asks AI systems to respond to input data that is low-quality or beyond the role the system was designed for, or puts too much weight on AI results absent human review, it will lead agencies and personnel astray. In the homeland security context, this will risk misuse of vital resources and diverting focus away from genuine threats. It also risks innocent individuals being unjustly subject to investigation, surveillance, arrest, and other deprivation of rights.

Beyond addressing risk of error and overreliance, it's also vital to take on the dangers of AI being used in a manner that undermines our democratic values. Facial recognition surveillance has already been weaponized in the United States to monitor peaceful protesters,[1] a commonly-employed tactic in China, Russia, and Iran that should never occur here.[2] Predictive policing has been shown to undermine due process rights and endanger innocent individuals.[3] The public has little insight into whether these types of disturbing uses have also occurred in national security contexts, or if adequate safeguards exist to prevent them. Greater transparency and oversight is needed to ensure AI does not undermine democratic values.

Question 2a. Pursuant to Executive Order 13960: "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," Federal agencies are required to create and make publicly available an inventory of non-classified and non-sensitive AI use cases, to the extent practicable and in accordance with applicable law and policy. DHS has made use cases across the Department publicly available on its website.

How has, or can, this public inventory shape industry AI efforts going forward?

Answer. The public inventory is a positive step for promoting necessary oversight of AI systems, and ensuring responsible use. A comprehensive inventory will also impact industry AI efforts by highlighting relevant needs and preferred-use scenarios. However, for this public inventory to be effective, it needs to account for the comprehensive set of agencies' uses of AI. The current Department of Homeland Se-

[1] See, Joanne Cavanaugh Simpson and Marc Freeman, "South Florida Police Quietly Ran Facial Recognition Scans to Identify Peaceful Protestors. Is That Legal?", *Sun Sentinel,* June 26, 2021, *https://www.sun-sentinel.com/2021/06/26/south-florida-police-quietly-ran-facial-recognition-scans-to-identify-peaceful-protestors-is-that-legal/*.

[2] For additional details, please see Section III of my written testimony, *https://cdt.org/wp-content/uploads/2024/05/Jake-Laperruque-5-22-24-AI-Hearing-Written-Testimony.pdf.*

[3] See, Pranshu Verma, "The never-ending quest to predict crime using AI," *Washington Post,* July 15, 2022, *https://www.washingtonpost.com/technology/2022/07/15/predictive-policing-algorithms-fail/;* see also, Matt Stroud, "Heat Listed," *Verge,* May 24, 2021, *https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list;* see also, Aaron Sankin and Surya Mattu, "Predictive Policing Software Terrible At Predicting Crimes," *Markup,* October 2, 2023, *https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes*.

curity ("DHS") inventory[4] contains disturbing gaps and omissions that indicate this is not the case. For example, its description of Immigration and Custom Enforcement's ("ICE") use of facial recognition is limited to Homeland Security Investigations, when public reporting has confirmed uses for general immigration enforcement.[5] Similarly, the inventory only describes Custom and Border Protection ("CBP") use of facial recognition in terms of the Biometric Entry-Exit program, but excludes any mention of use of this AI tool by Border Patrol agents in field settings. Until public inventories provide a genuine overview of all AI systems, they will not provide the transparency and oversight this system was designed for.

The public inventory should also strive to provide greater information on how broadly AI systems are available to personnel and nature of their use. Understanding how AI systems are deployed can have a significant impact on the AI industry, and whether stakeholders and the public deem such use appropriate, in need of greater rules and safeguards, or believe it should be discontinued. For example, the DHS Inventory describes "Mobile Device Analytics" as one AI system used by ICE for "identifying pertinent evidence, relationships, and criminal networks from data extracted from cellular phones" as well as "object detection (such as firearms, drugs, money, etc.)" This tool could supercharge warrantless surveillance if combined with DHS's database of cell phones searched and copied during border searches: Each year CBP downloads information (such as text messages, photos, videos, communications logs) from up to 10,000 phones into a central database, where such data is stored for 15 years and accessible by 2,700 personnel.[6] Are Mobile Device Analytics AI systems applied to this database? If so, how frequently, by how many personnel, and for what range of purposes? In order to be effective, the public inventory should not simply list types of AI systems deployed, but also give insights into manner of use.

Finally, the Government should take steps to provide transparency on AI uses within Classified and Sensitive settings as well. Agencies should strive to declassify as much relevant information as possible to offer public overviews and summaries of AI uses, with full descriptions provided to Congress. Additionally, the steps outlined in my written testimony will promote transparency and oversight even for Classified uses. Mandatory declassification review of key documents, such as agency rules and AI efficacy assessments, will aid public understanding and facilitate responsible use. Congress' required declassification review and required publication of significant FISA Court opinions demonstrates the feasibility and value of such a system. An AI Oversight Board can also carefully examine use within Classified settings, promote public awareness to the best degree possible, and provide recommendations directly to agencies in areas where details cannot be disclosed.

Question 2b. Are there any gaps in the DHS use case inventory that could be addressed with AI-based solutions?

Answer. The Center for Democracy & Technology does not have any specific AI use cases it recommends adding to the current DHS inventory. The Government should always strive to improve systems and harness technological innovations in pursuit of this goal, but do so in a responsible manner that prioritizes civil rights and civil liberties. As DHS and other agencies consider additional AI systems, it should prioritize examining efficacy, reviewing civil rights and civil liberties risks, and developing appropriate rules and safeguards before acquisition and implementation. Our recent report offers detailed recommendations on effective procurement practices for AI systems.[7]

Question 3a. Many companies are embracing generative AI. However, Gartner found that there is still a significant gap for AI adoption within enterprises that is

[4] The full Department of Homeland Security public inventory, "Artificial Intelligence Use Case Inventory," is available at *https://www.dhs.gov/data/AI_inventory.*

[5] Drew Harwell, "FBI, ICE find State driver's license photos are a gold mine for facial-recognition searches," *Washington Post,* July 7, 2019, *https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/;* see also, Nina Wang, Allison McDonald, Daniel Bateyko & Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century,* Centeron Privacy & Technology at Georgetown Law (2022) ("ICE has used face recognition technology to search through the driver's license photographs of around 1 in 3 (32 percent) of all adults in the U.S.").

[6] Jessica Lyons, "US border cops harvest info from citizens' phones, build massive database," *Register,* September 15, 2022, *https://www.theregister.com/2022/09/15/wyden_cbp_phone_database/.*

[7] Hannah Quay-de la Vallee, Ridhi Shetty, and Elizabeth Laird, *The Federal Government's Power of the Purse: Enacting Procurement Policies and Practices to Support Responsible AI Use, The Center for Democracy & Technology* (2024), *https://cdt.org/insights/report-the-federal-governments-power-of-the-purse-enacting-procurement-policies-and-practices-to-support-responsible-ai-use/.*

largely driven by challenges "estimating and demonstrating the value of AI projects."

Do you think the potential of generative AI, as depicted by the media, is overhyped or accurate? Why or why not?

Answer. Overreliance on AI is a serious risk, not only in terms of general automation bias—in which individuals tend to place excess trust in answers from automated systems—but also in expecting systems to yield fruitful results even when given poor quality input data or used in a manner beyond their designed purpose. In reality, AI systems are only as good as the data they are given, and garbage in leads to garbage out. And even when AI systems are well-designed, given quality input data, and used properly, human review from properly-trained individuals is essential to ensuring AI is not relied on excessively.

As I described in my testimony, facial recognition shows the dangers of failing to heed these fundamental lessons for responsible use: Vendors sometimes frame their products as near-infallible, and urge law enforcement to rely on low-quality images that are much more prone to misidentifications. Police departments have been documented engaging in baseless misuses of the technology, using CGI-generated images, sketches, and lookalikes in place of individuals' actual faces. Failure to assess and corroborate results has led to numerous individuals being improperly arrested and jailed.[8]

These examples show the dangers of overhyping AI. If we do not properly account for its limits and act accordingly, it will cause serious and concrete harm to Americans' lives.

Question 4. How do we ensure that the future of AI policy—which will impact the entire economy and national security—is not dominated by Big Tech?

Answer. There are several steps the Federal Government can take now to help ensure that the resources necessary to take advantage of powerful AI are available broadly, rather than concentrated with a small set of powerful technology companies.

First—as detailed in CDT's recent comments to the National Telecommunications and Information Administration in its proceeding on the risks and benefits of large AI models with publicly-available weights—ensuring a vibrant ecosystem of openly-published models as a competitor to closed, centrally-hosted services will help combat market concentration in AI, much as open-source software has been an engine of innovation and competition in other technologies for the past 3 decades.[9] Therefore we urge Congress, as we urged the Commerce Department, to support the development of such an ecosystem including by preserving the open scientific discourse it requires, as well as to be wary of proposals to broadly restrict the ability to publish AI models and research based on speculative risks.[10]

Second, the Government can help democratize the resources necessary to do AI science—including research that would help developers build AI more responsibly and contribute to a safer and more competitive open model ecosystem—by funding new research and development activities and institutions. For example, the CREATE AI Act (H.R. 5077) and the Future of AI Innovation Act (S. 4178) both would Congressionally authorize 2 new valuable efforts to provide more public resources for AI model development and testing including for safety and governance purposes. Those two efforts, respectively, are the National AI Research Resource at the National Science Foundation and the AI Safety Institute at the National Institute of Standards and Technology, each of which CDT supports.

Third, we should prioritize responsible procurement policies, given impact that the U.S. Government's role as a major purchase will have on the industry. The United States Government awarded over $2 billion in contracts to private companies that provide AI-reliant services in fiscal year 2022, with total spending on AI increasing nearly 2.5 times since 2017.[11] Government procurement practices should

[8] For additional details, please see Section III of my written testimony, *https://cdt.org/wp-content/uploads/2024/05/Jake-Laperruque-5-22-24-AI-Hearing-Written-Testimony.pdf.*

[9] Kevin Bankston, Center for Democracy & Technology, "CDT Comments to the National Telecommunications and Information Administration on Dual-Use Foundation Artificial Intelligence Models with Widely-Available Model Weights as per Section 4.6 of the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," Docket No. 240216–0052, March 27, 2024, *https://cdt.org/insights/cdt-comments-to-ntia-on-open-foundation-models/*.

[10] See also Letter of Civil Society Organizations and Academics to Commerce Secretary Raimondo, March 25, 2024, *https://cdt.org/insights/cdt-joins-mozilla-civil-society-orgs-and-leading-academics-in-urging-us-secretary-of-commerce-to-protect-ai-openness/*.

[11] Hannah Quay-de la Vallee, Ridhi Shetty, and Elizabeth Laird, *The Federal Government's Power of the Purse: Enacting Procurement Policies and Practices to Support Responsible AI Use,* The Center for Democracy & Technology (2024), *https://cdt.org/insights/report-the-federal-gov-*

be tailored to carefully assess AI quality, ability to meet agency needs, and comportion with policy safeguards and limits. This will facilitate AI developers rising on merit, rather than succeeding simply due to status as large incumbent actors. CDT has recommended a number of actions to support responsible procurement practices, including measures to support responsible AI considerations at the acquisition planning stage, more effective pre-award vendor evaluation, and proper post-award vendor monitoring both from within agencies and via oversight by Congress, the Government Accountability Office, and the Office of Budget and Management.[12]

Question 5. What do you think the broader U.S. AI ecosystem can do to maintain its lead in generative AI over China, which is currently heavily regulating its AI?

Answer. It's vital that we evaluate AI through the proper lens: Winning the "AI Arms Race" does not simply mean the fastest deployment on the broadest scale, it means ensuring that AI technologies promote democratic society and values. As I detailed in my written testimony, China's weaponization of AI to promote authoritarianism and undermine individuals rights provides a stark warning: The government uses facial recognition to hamper protests, oppress its Uygher minority, and conduct pervasive surveillance of low-level offenses like jaywalking to build a "Big Brother Is Always Watching" mentality.[13] The United States must take a values-based approach to its development and deployment of AI, and ensure that it aids civil rights and civil liberties.

We should also prioritize transparency in systems and Government applications of AI; this will not only ensure responsible use, but also promote efficacy and innovation. We should prioritize open-source systems, as well as transparency in how various AI technologies are developed and used both in and outside Government. Doing so will facilitate public engagement and input from a broader set of experts and stakeholders. American innovation has always thrived by fostering a marketplace of ideas, and AI technologies are no exception. If we wish to prevail over our strategic rivals, the United States must ensure that AI development occurs in an open environment, and with the goal of supporting democratic values.

Question 6. As deepfakes proliferate and become more believable due to advances in AI, what should be the relationship between organizations that use AI in the public and private sectors, including social media companies, to detect mis-, dis-, and mal-information?

Answer. More needs to be done to combat disinformation, especially as AI technologies such as deepfakes will both allow disinformation to be produced more easily, spread more quickly, and mislead individuals more convincingly. Social media companies should invest more in watermarking and content detection methods to ensure that AI-generated content is properly flagged as quickly as possible. Beyond direct investment, social media companies should support independent research by providing access to relevant data and information, as my colleague outlined in a comment last month to the National Institute of Standard and Technology.[14]

Companies should also work to ensure that trust and safety mechanisms can continue to operate at scale even as AI facilitates more rapid production and dissemination of disinformation. In employing AI as a defensive measure to combat disinformation, these efforts should account for added challenges in evaluating different forms of content and content in different languages. CDT research has demonstrated how automated content moderation in general, and in particular in regard to multimedia and multilingual content, has serious limits.[15]

ernments-power-of-the-purse-enacting-procurement-policies-and-practices-to-support-responsible-ai-use/.

[12] Id.

[13] Paul Mozur, "In Hong Kong Protests, Faces Become Weapons", *N.Y. Times,* July 26, 2019, *https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html;* Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority", *N.Y. Times,* Apr. 14, 2019, *https://www.nytimes.com/2019/04/14/technology/chinasurveillance-artificial-intelligence-racial-profiling.html;* Alfred Ng, "How China Uses Facial Recognition to Control Human Behavior", CNET, Aug. 11, 2020, *https://perma.cc/P6Y3-U7XV.*

[14] Kate Ruane, "Comment on NIST AI 100–4," The Center for Democracy & Technology, May 31, 2024, available at *https://cdt.org/wp-content/uploads/2024/06/5.31.24-CDT-Comment-on-NIST-AI-100-4.pdf.*

[15] See, Natasha Duarte and Emma Llansó, *Mixed Messages? The Limits of Automated Social Media Content Analysis,* The Center for Democracy & Technology (2017), *https://cdt.org/insights/mixed-messages-the-limits-of-automated-social-media-content-analysis/;* see also Dhanaraj Thakur and Emma Llansó, *Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis,* The Center for Democracy & Technology (2021), *https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/;* see also Gabriel Nicholas and Aliya Bhatia, *Lost in Translation: Large Language Models in Non-*

Continued

We should also strive to borrow past models that have proven successful. Over the past decades the United States has built robust systems to aid cybersecurity by facilitating sharing of useful information among private-sector entities, and between the private sector and the Government. Creating similar infrastructure to promote rapid dissemination of relevant information to combat AI-generated disinformation and threats could be beneficial as well.

○

English Content Analysis, The Center for Democracy & Technology (2024), *https://cdt.org/insights/lost-in-translation-large-language-models-in-non-english-content-analysis/*.