USING CUTTING-EDGE TECHNOLOGIES TO KEEP AMERICA SAFE

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

JUNE 22, 2023

Serial No. 118–47

Printed for the use of the Committee on Oversight and Accountability

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

U.S. GOVERNMENT PUBLISHING OFFICE
52–826 PDF WASHINGTON : 2023

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

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

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

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

CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director
CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

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

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

C O N T E N T S

WITNESSES

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

INDEX OF DOCUMENTS

Documents are available at: docs.house.gov.

USING CUTTING–EDGE TECHNOLOGIES TO KEEP AMERICA SAFE

Thursday, June 22, 2023

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

The Subcommittee met, pursuant to notice, at 1:05 p.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Timmons, Greene, Luna, Langworthy, Burlison, Connolly, and Lynch.

Ms. MACE. Good afternoon, everyone.

The Ranking Member, Connolly, is on his way, but the Subcommittee on Cybersecurity, Information Technology, and Government Innovation will now come to order.

We want to welcome everyone who is here this afternoon. We have almost every seat full.

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

Good afternoon and welcome to this hearing on the Subcommittee on Cybersecurity, Information Technology, and Government Innovation. Today, we are going to explore the use of cutting-age technology to protect America's citizens and its borders. The innovations we will discuss also help to protect border security officials, law enforcement officers, and military personnel who put their lives on the line each and every day to keep the rest of us and our Nation safe.

We will see firsthand today some of the new hardware that has been deployed. We will hear examples of current-use cases by Federal agencies and what sort of innovations could be coming around the corner. Many security-related innovations are first acquired by the U.S. military. These are then adapted and adopted by other parts of government, such as U.S. Border Patrol and other law enforcement.

We will hear today how robotics, scanners, and drone technology are being put to good use at the border. We will also discuss what may be coming tomorrow.

At this Subcommittee's first hearing this year, we heard from experts about how recent developments of in AI, or artificial intel-

ligence, will change the way we live and work. They said AI could revolutionize many fields. One such field is security operations.

Former Google CEO, Eric Schmidt, who testified before this Subcommittee, testified how critical it is to our Nation's defense that we maintain our edge over China in AI development. Our military has for years worked to find ways to harness AI to enhance our war-fighting capabilities.

And I have a message for Elon Musk today: We are not going to pause AI development or research or innovation for six months because China is not going to pause its research or its AI development at any time or any moment in the near or distant future. We want to make sure we stay ahead of those who may be adversaries now or in the future.

But the reality is that the capabilities of robots, drones, scanners, and other security hardware may be supercharged by advances in AI, and the implications of that go well beyond war-fighting. That is why I recently wrote to the Department of Homeland Security, Secretary Mayorkas, to find out how his agency intends to use AI to stop the flow of illegal immigrants and drugs across the southern border.

I have also personally spoken with Border Patrol officials about how they are using biometrics at the border, how artificial intelligence can help enhance the effectiveness of our existing technology.

Guarding the border is hard. It is dangerous work. It often requires relocating to a remote area, increasing the burden this can put on morale or the lax policies and weak leadership of our current administration. The leadership of the Department of Homeland Security should be as invested in the Border Patrol's mission as are the dedicated agents patrolling the southern border, but, unfortunately, today that is not the case, and it is a situation we must change.

Meanwhile, it should surprise no one that the border patrol is struggling mightily with recruitment and retention, and in the district that I represent, South Carolina's First congressional District in the low country of South Carolina, we actually have a Border Patrol training academy at FLETC. And we are very proud of the work that we do there, but we also know how hard and difficult it is to recruit and retain those who want to work on our Border Patrol.

Technology alone cannot solve many of the challenges we face today, but it can help alleviate the demand on manpower by providing each individual agent the tools to enable them to do their job more effectively and, even in some cases, more safely.

In Congress, we can help make that happen. We can help ensure the most effective new security technologies the private sector develops gets into the hands of Border Patrol agents and other Federal law enforcement and law enforcement agencies. That requires ensuring Federal agencies are acquiring the best technologies developed by the private sector in a timely and cost-effective manner. It means ensuring agencies are working with small, nimble innovators, as well as large, established contractors. It means ensuring red tape and other entry barriers are not preventing newcomers from competing to provide security products and services.

I am pleased that we have witnesses here today who have volunteered to come forward and share with us directly some of the hardware that is currently being deployed to keep our Nation safe, and I honestly, personally, am very much looking forward to seeing some of the demos and the technology that you all brought before this Committee today.

It is my hope this hearing will provide Members a better appreciation of the value proposition these technologies bring today, as well as their future potential.

And, with that, I am going to go ahead and skip to our witnesses while we wait on the Ranking Member, Connolly.

Ms. MACE. So, I am pleased to introduce our witnesses for today's hearing. Our first witness is Mr. Ryan Rawding, Vice President of Business Development at Pangiam.

Our second witness is Mr. Wahid Nawabi, Chairman, President, and CEO of AeroVironment.

Our third witness is Dr. Gavin Kenneally, Chief Executive Officer at Ghost Robotics.

Our fourth witness is Dr. Benjamin Boudreaux, Policy Researcher and Professor of Policy Analysis at the Pardee RAND Graduate School at RAND Corporation.

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

So, pursuant to Committee Rule 9(g), the witnesses, we would ask you to please stand and raise your right hands.

This is where it gets real.

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

Let the record show that the witnesses all answered in the affirmative.

We appreciate all of you being here today and look forward to your testimony. I would like to remind the witnesses that we have read your written statements, and they will appear in full in the hearing record. Please limit your oral statements this afternoon to five minutes.

As a reminder, please press the button on your microphone in front of you so that it is on, and the Members can hear you. When you begin to speak, the light in front of you will turn green. After four minutes, the light turns yellow. When you hit five, it is red. That means stop. We would just ask that you wrap up your comments.

You all may sit down.

And I would first like to recognize Mr. Rawding to please begin your opening statement.

STATEMENT OF RYAN RAWDING
VICE PRESIDENT OF BUSINESS DEVELOPMENT
PANGIAM

Mr. RAWDING. Thank you.

Chairwoman Mace, Ranking Member Connolly, and distinguished Members of the Subcommittee, thank you for the opportunity to appear today on behalf of Pangiam to discuss cutting-edge technologies to keep America safe.

My name is Ryan Rawding, and I am Vice President of Business Development at Pangiam, a trade and travel technology company.

Before my tenure at Pangiam, I served as a CBP officer within the office of field operations for 13 years, with a significant portion spent at CBP's national targeting center. During my time at the NTC, I drove many of the requirements and multiple targeting—for multiple targeting and vetting systems, including the implementation of facial recognition. I collaborated closely with foreign counterparts across the globe and established NTC's foreign encounter team.

I am here today on behalf of Pangiam to share with the Subcommittee my views and experience of how CBP has leveraged emerging technology in identity resolution in response to U.S. Border Patrol's recent migrant surge, resulting in the creation of the mobile intake application.

In the summer of 2021, the U.S. experienced a significant rise in apprehensions at the southern border, surpassing over 250,000 in December 2022 alone. This surge has hindered Border Patrol's ability to identify and rapidly process individuals encountered between the ports of entry.

Prior to the introduction of mobile intake, border patrol agents in the field relied on a manual process to document encounters. This resulted in a lack of immediate identity resolution and threat identification, led to data integrity issues, and time wasted in duplicative efforts between field and processing agents.

To tackle these challenges, CBP collaborated with Pangiam to develop the mobile intake app. This innovative solution harnesses facial recognition technology, enabling Border Patrol agents to biometrically enroll migrants using their government-issued smartphones at the point of encounter.

Mobile intake utilizes AI and computer vision to capture the subject's face and leverages optical character recognition to extract biographical information from documents and track migrants properly. The captured photo is then cross-verified against previous CBP encounters, allowing agents to confirm the identity and access prior apprehension data. The app also allows agents to identify and track families from the point of encounter, assisting with family unification.

Since January of this year, field agents are instantly alerted if the enrolled individual has a record on a government watch list, providing an additional layer of security to those agents.

Once a group has been captured through the application, the agent can update the geolocation for accurate tracking, then submit the data package for instant ingestion into the Border Patrol case processing system. In the event the agent is in rough terrain and without connectivity, a peer-to-peer functionality exists in that the agent can pass the data package from one device to another via secure WiFi so the transporting agent can submit the group once connectivity has been reestablished.

These proactive approaches enable the receiving station to anticipate arrivals, efficiently allocate resources, expedite processing, and ensure proper care for individuals within CBP custody. The successful mobile intake is attributed to the strategic approach led

Border Patrol and the Office of Information Technology, with its contracting staff.

Comprehensive requirements were accurately defined through active engagement with the frontline field operators and subject-matter experts. Following commercial best practices, we developed a minimal viable product to CBP after 120 days of active development in March 2022. It has since been expanded to all Border Patrol sectors with over 13,000 agents using the application to enroll more than 750,000 migrants to date.

As you can see, the mobile intake app delivered notable advantages for Border Patrol. It enhances agent safety through identity resolution, and safeguards migrants by keeping families intact and identifying potential threats.

As countries in Central and South America strengthen their border security measures and establish identity verification processes, manual collection methods have presented the same challenge that Border Patrol has previously faced. One potential solution is to provide foreign governments with a biometric enrollment capability, such as the mobile intake app, in return share this information back with CBP for advanced screening of northbound migrants.

In closing, Chairman Mace, Ranking Member, and esteemed Subcommittee Members, I am grateful for the Subcommittee's attention to the significant potential that these technologies hold for improving border security, and I look forward to your questions today.

Ms. MACE. Thank you, Mr. Rawding.

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

STATEMENT OF WAHID NAWABI
CHAIRMAN, PRESIDENT AND CHIEF EXECUTIVE OFFICER
AEROVIRONMENT

Mr. NAWABI. Chairwoman Mace, Ranking Member Connolly, and distinguished Members of the Committee, I am Wahid Nawabi, Chairman, President, and CEO of AeroVironment, Inc. We are a 52-year-old technology company, publicly traded on the NASDAQ.

I was born and raised in Afghanistan. As a 14-year-old teenager, I escaped Afghanistan with my three younger sisters, traveling for two months from Kabul, Afghanistan, through Pakistan to New Delhi, India. We were reunited with my parents in New Delhi. I legally immigrated to the United States at age 15, became a U.S. citizen, and started a new life as an American, learning English, finishing high school and college, becoming an electrical engineer.

I am an example of a legal immigrant who pursued the American Dream. I feel a personal obligation and consider it my duty to help improve the security of our Nation and defend our values not only in the United States, but around the globe.

I am grateful for the opportunity today to represent the 1,300 employees of AeroVironment and discuss with you our current and future vision of intelligent robotic systems and how they will enhance our safety and security.

AeroVironment's robotic systems enable the success and assure the safety of government and commercial customers. We are a global leader in unmanned aircraft systems, unmanned ground vehicles, loitering munition systems, and high-altitude pseudo-sat-

ellites. We are a large supplier of unmanned systems to the United States Department of Defense, providing products to all the military services and U.S. Special Operations Command, as well as the U.S. Department of State, Justice, and Homeland Security.

Additionally, our small, unmanned aircraft systems are employed by more than 50 allies around the globe. We have over a dozen facilities across the country. All our products are manufactured in the United States, except our unmanned ground vehicles, which are made in Germany.

In 2021, AeroVironment celebrated its fiftieth anniversary. Over the last half-century, we have been innovation pioneers, pushing the boundaries of what is possible and delivering advanced solutions to support our government and commercial customers.

In the 1980's, AeroVironment created the first portable, hand-launched drone for information collection and transmission. Beginning in the 2000's, the U.S. Department of Defense selected AeroVironment's small, unmanned aircraft systems for multiple programs of record. In 2021, AeroVironment developed critical components for the Mars ingenuity helicopter, the first powered aircraft flight on another planet and the 2021 Robert J. Collier award winner for the greatest achievement in aeronautics or astronautics in America.

Most recently and over the last year, AeroVironment's innovative solutions have helped Ukraine defend itself from Russia, providing critical intelligence, reconnaissance, surveillance, and precision strike capabilities. AeroVironment's products are not only critical on the battlefield but also greatly enhance domestic capabilities, such as law enforcement, Border Patrol, and natural disaster relief.

Future missions for intelligent robots, integrated with artificial intelligence and autonomy, not only require imagination. Systems operating on the ground and up to the stratosphere will enhance global communication, transportation, infrastructure and agriculture inspection, weather monitoring, and provide disaster preparedness and relief.

Our solar-powered, high-altitude pseudo-satellite can provide a global broadband telecommunications network, weather monitoring for organizations such as NOAA and FEMA, as well as space domain awareness. Powered entirely by solar arrays, it is designed to stay aloft for up to six months in the stratosphere.

Government and commercial customers are only just beginning to harness the potential of this revolutionary and cost-effective capability.

AeroVironment continues to develop unmanned systems with computer vision and machine learning capabilities, which can navigate autonomously on its own, sense, analyze, and identify itself of interest—items of interest, reducing operator workload and increasing situational awareness and safety. We constantly evaluate and integrate new capabilities into our current and future products to assure we stay ahead of our competitors and our Nation's adversaries.

I would like to share a short video showcasing a few of our current and future systems employed by our government and commercial customers. And, if you do not mind, please play the short video.

[Video played.]

This is our Puma system that you see on the right side displayed here on your left hand that can be launched off. This is our stratospheric solar airplane that takes off from a runway in Spaceport, New Mexico. It has a wingspan that is longer than an Airbus A380. It goes up to the stratosphere and stays there for six months at a time, and it can do all sorts of missions.

Our ground robots are used for EOD purposes. The Capitol Hill Police uses them here in the Capitol Hill district. And, of course, our object identification and computer vision can identify very specific objects in very cluttered large swaths of imagery. You can give the computer that image, and it will find out Wahid Nawabi in that very cluttered space.

So, thank you again to the Committee for the opportunity to be here today. I invite each of you to visit AeroVironment facilities across the country.

And I welcome your questions.

Ms. MACE. Thank you, Mr. Nawabi.

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

STATEMENT OF GAVIN KENNEALLY
CHIEF EXECUTIVE OFFICER
GHOST ROBOTICS

Mr. KENNEALLY. Chairwoman Mace, Ranking Member Connolly, and Members of this Subcommittee, thank you for the invitation and the opportunity to testify before the Cybersecurity, Information Technology, and Government Innovation Subcommittee.

My name is Gavin Kenneally, and I am the CEO of Ghost Robotics, which I cofounded with CTO Avik De in 2015. Avik and I met while completing our Ph.D.s at the University of Pennsylvania and started the company based on our shared commitment of creating highly responsive and agile legged robots for real-world applications.

Through our research, we discovered that we could design a legged robot with less complex hardware and more sophisticated software using motors to directly feel the ground through the legs. Working closely with our early customers, we developed a scalable robot that could meet government, as well as commercial needs, and have created this machine, the Vision 60.

[Demonstration.]

Mr. KENNEALLY. Great. Thank you very much, Michael.

Mr. CONNOLLY. It looks like my high school algebra teacher.

Mr. LYNCH. Like an Avengers movie right now.

Mr. KENNEALLY. Our robot is able to overcome more challenging terrain than similarly sized wheeled or tracked machines. It can move on rocks, sand, hills, ice, and snow, and can climb up and down stairs. If our robot falls or gets knocked over, it can even operate upside down or can right itself to complete the mission.

The Vision 60 can operate in austere environments, from minus 40 to 130 degrees Fahrenheit. The robot leads its class in endurance and can walk continuously for over six miles on a single charge. When the battery runs low, the robot can automatically recharge itself by going back to a wireless charging station.

The Vision 60 is currently used by many branches of the Department of Defense. It performs perimeter security at eight Air Force bases throughout the country. The robot's ability to traverse difficult terrain in all weather and in extreme temperatures makes it ideal for environments found along the U.S. southern and northern borders. In addition, we have done field testing with the Science and Technology Office of the Department of Homeland Security.

The Vision 60 platform has many features that are crucial for national security and protection purposes. It has onboard color cameras and microphones, as well as twenty-two pounds of additional capacity for other payloads as necessary. The robot can interface with standard off-the-shelf sensors, such as pan-tilt-zoom, thermal or infrared cameras, and then either analyze and do anomaly detection on the robot itself or stream the video back to the controller or base station.

The robot can also interface with many chemical, biological, radiation, and nuclear sensors to identify all kinds of dangerous or toxic substances from afar.

When used to traverse difficult terrain found along the U.S. borders, our Vision 60 robot, equipped with appropriate sensors, can save lives. For example, patrolling robots with a Raman Spectroscopy sensor could be used to improve drug trafficking detection. This is an invaluable asset, given that, according to the U.S. Drug Enforcement Administration, fentanyl is the leading cause of death for Americans under the age of 50, and the majority of it flows into the U.S. across the southern border.

In addition, given that several hundred migrants die every year near the southern border from drowning or heat-related causes, a thermal camera could be equipped on the robot and used to identify them before it is too late.

There are many other such beneficial applications from using these robots for data collection and as communication nodes, which will emerge with the continued collaboration between Ghost Robotics and the Department of Defense and other government agencies.

Thank you. And I look forward to your questions.

Ms. MACE. Thank you.

The robot runs, too, right?

Mr. KENNEALLY. It does, yes.

Ms. MACE. It jogs.

Mr. KENNEALLY. It does, yes. It can run at two-and-a-half meters per second, about a 10 or 11-minute mile.

Ms. MACE. Yes.

Thank you, Dr. Kenneally.

I would like to now recognize Dr. Boudreaux for your opening statement.

(MINORITY WITNESS)
STATEMENT OF BENJAMIN BOUDREAUX
POLICY RESEARCHER AND PROFESSOR
OF POLICY ANALYSIS
PARDEE RAND GRADUATE SCHOOL, RAND CORPORATION

Mr. BOUDREAUX. Chairwoman Mace, Ranking Member Connolly, and Members of the Committee, good afternoon, and thank you for the opportunity to testify today.

I am a policy researcher at the RAND Corporation, a nonprofit and nonpartisan research organization that manages federally funded research and development centers for the Department of Homeland Security and the Department of Defense. Before joining RAND, I served as a foreign affairs officer at the Department of State, and I earned a Ph.D. in philosophy with a focus in political philosophy and ethics.

Today, I will concentrate my comments on the importance of ensuring that government technology deployments serve the interest of the public.

The U.S. Government frequently deploys emerging technologies that directly affect Americans. For example, DHS uses artificial intelligence and other technologies that can recognize human faces, track mobile phone location, and analyze social media activity. These technologies are purported to bring a variety of benefits to government missions. For instance, by increasing the speed and accuracy of decision-making, such as in the global entry trusted traveler program.

However, the potential of government use of emerging technologies to keep Americans safe is subject to several important considerations. This includes an accurate assessment of the benefits and risks of the technology and the public's trust that these rapidly advancing technologies are used responsibly.

Key stakeholders, such as Members of Congress from both parties, technology companies, and AI researchers have raised concerns about government use of emerging technologies. These concerns include risks that government applications violate privacy and civil liberties, exacerbate inequity, and lack appropriate transparency and other safeguards.

An essential element to help ensure that government use of technology serves the public interest is to better understand the public's perception of their use. Public perception is important for several reasons, such as to establish trust in and the legitimacy of government, to facilitate necessary funding and legislative support from Congress, and to foster collaboration with technology companies and operational partners. It is also crucial that the U.S. Government understand the perspectives of different demographic groups, especially those voices that are marginalized, to recognize the disparate impact across communities.

Greater understanding about how the public views potential benefits and risks of technologies can inform multiple stages of the technology acquisition and deployment lifecycle.

Drawing on RAND research conducted for DHS, I suggest three recommendations for the government when it is considering deploying new technology. First, the government can take steps to ensure that longstanding core American values apply to new technologies. The U.S. Government is committed to values such as privacy and civil liberties, equity and nondiscrimination, and oversight and accountability.

Even if newly available technologies, including AI systems and advanced robotics, assist in government missions, the protection of core values is also essential for keeping Americans safe.

Second, details of the technology and specific government application matter for responsible deployment. For instance, tech-

nologies used in sensitive public spaces, such as schools using AI to surveil on students, might pose increased risks and thereby warrant greater care. Some emerging technologies, such as large language models, have capabilities beyond what even the technology developers themselves anticipate, yet, according to the Government Accountability Office, some technologies are being deployed across government without consistent approaches to even track which technologies agencies are using.

Congress can help ensure that agencies take a coherent and a risk-informed approach and that government end users are precise about their goals for a technology, the specific context of use, and their relevant authorities.

Third, new technology deployments are an opportunity for public engagement. The government should collaborate with stakeholders and communities to ensure that technology is used in ways the public supports. DHS has recently sponsored RAND research to identify methods to assess public perception, such as conducting nationally representative surveys of the public. This type of public perception research, supplemented with additional surveys, focus groups, and community partnerships, should be routinely integrated into the technology, acquisition, and development pipeline. This will help the government anticipate potential issues, engage affected communities, and build the public's trust.

I thank the Committee for this opportunity to testify, and I look forward to your questions.

Ms. MACE. Thank you, Dr. Boudreaux.

We have just been called for votes, but my esteemed colleague from Virginia wants to give a brief opening remark.

So, I'll recognize Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chair.

And thank you to our panel for being here today.

I will be brief. You and I have agreed that we will have a conversation offline, but I want to remind the Chair that our first discussion about the future course of this Subcommittee was in February, in Munich. The Chair indicated to me she had 17 hearings planned, and I indicated I would be supportive.

However, we wanted to continue to do the bread and butter that we have done on this Subcommittee with respect to FITARA and the modernization of IT in the Federal Government. We made an agreement about having a hearing.

It is now June, almost July. We have always had, in eight years since we passed FITARA on a bipartisan basis, two hearings a year on the implementation of FITARA. We created a scorecard, and, according to GAO, that scorecard has helped save $25 billion. There are not many programs or pieces of legislation in Federal history that save money, let alone $25 billion.

I am always open to updating and modernizing tools we have to measure progress. What I am not open to is not having the oversight hearing at all, and I hope the Chair and I can work it out for the sake of harmony on this Subcommittee.

I have worked with Darrell Issa, Mark Meadows, Trey Gowdy, Jody Hice throughout the years on a bipartisan basis on this subject matter and on specifically those hearings on that scorecard.

So, I look forward to working with the Chair and having offline discussions, but I want to make it very clear: Waiting until December to have that hearing is not something acceptable to this side of the aisle. So, I hope we can work it out and move forward in a cooperative fashion.

I thank the Chair.

Ms. MACE. Thank you, Mr. Connolly.

And now that they have called votes, we are going to recess briefly for our votes, and the hearing will resume after our last vote.

Thank you for your patience this afternoon.

[Recess.]

Ms. MACE. All right. We are now back in order this afternoon. Thank you for your patience. We will reconvene.

And I would now like to recognize myself for five minutes to ask you gentlemen a few questions this afternoon. I would like to first start with Mr. Nawabi.

In talking about AI and currently the role AI plays on your company's unmanned drones and unmanned ground robots, et cetera, what sort of role does AI play? How do you anticipate AI now and in the future playing a larger role in these types of technologies?

Mr. NAWABI. Ms. Mace, so the AI is a pretty broad set of capabilities and spectrum of—imagine the most elementary capabilities all the way to the very complex missions.

You could argue that today even, in the last decade, we have had some level of autonomy built into our drones. So, in most of these drones that you see, and they are not—the operator or the pilot is not manually flying it most of the time. Most of the time the pilot is basically telling the UAV to go from here to here on a map by just touching on a tablet, and then the UAV and the software algorithms on board, the auto pilots, actually flies it. It tells it what to fly—how to fly to get there. So, there is some level of automatic flight and control already built in.

And we just launched another sort of enablement for the Puma systems called our visual navigation system. What that does is—almost all drones that are made rely on GPS for knowing exactly where they are and relative to the space they are in, and then to figure out where to go.

So, an example such as in Ukraine where there is a lot of jamming, you cannot really rely on GPS. So, the module that we just launched as an enhancement, it has algorithms in it that allows the sensors on board the drone to figure out where it is without having any GPS signals at all. And so that is another level of intelligence and autonomy that is built into it.

The video that I showed that showed a picture of a huge bay or a large swath of land, there are algorithms that we have developed that can actually recognize a specific object or asset, whether it could be a tank, a ship. You can even specifically tell it to look for a Russian tank or a specific object that you like.

And so that level of AI and capability keeps becoming more and more prevalent and more and more out there, and those are the things that we are working on. So, I see for the next several years to decades these capabilities to keep getting better and better and more and more features and capabilities will be adopted and provided to our customers.

Ms. MACE. And then my second and probably last question, because I have about two and a half minutes left, I would like each of you to spend 20 or 30 seconds, and that is a very short period of time, and it is a loaded question, but there have been a lot of concerns about AI and technologies, robotics, et cetera. There are some people that would see the robot dog, as I am going to call it, and think that that might be utilized, you know, years from now, not any time soon, against them.

And so, in thinking about some of the concerns, whether it is data security, cybersecurity, you know, the advent of AI is moving technology and cybersecurity threats in rapid pace.

So, just some really high-level thoughts in 20 to 30 seconds, sort of how do we prepare ourselves for that future. What are your concerns? How are we addressing those concerns, et cetera?

Mr. Rawding?

Mr. RAWDING. Thank you, Chairwoman.

In my experience, I think employing a lot of supervised machine learning models where in the Customs and Border Protection space the computers and machines are not ultimately making the decision, but they are giving risk-based scores where the agents and officers are able to ultimately make that determination.

And then kind of staying within that public-private partnership with academia, the government, and its contracting staff to make sure that all privacy concerns are met so that the people feel safe while we're employing these technologies.

Ms. MACE. Mr. Nawabi?

Mr. NAWABI. Thank you, Chairwoman Mace.

In general, all of our systems—we take cybersecurity and the security of our systems very seriously because it's a requirement by our customers, primarily for not only domestic applications but also for military.

One of the intentional decisions we made a long time ago was to develop a lot of our subsystems that go into these solutions all internally ourselves in the United States. So, there is already a significant level of security built into the software, into the design of the UAVs, and to making sure that we secure the system that it becomes more and more secure.

There are also some FAR clauses, the Federal Acquisition Regulations Act, that requires contractors, such as AeroVironment to be compliant, and there are several clauses in the FAR that does that.

In short, we take it seriously. We have done a lot of things in there, and we are going to continue to do a lot more. I think that what distinguishes us from a lot of other consumer players is this level of security and safety that we provide that is really going to make it a unique advantage for us and for a benefit for our customers.

Ms. MACE. Thank you.

I have run out of time now. We will come back if we can a few minutes at the end.

And I would like to yield five minutes to Mr. Lynch.

Mr. LYNCH. Thank you, Madam Chair.

First of all, I want to thank our panel members for your willingness to come before the Committee and share your expertise and

help us with our work. Thank you for the presentations that have been brought forward here. We appreciate that.

Mr. Boudreaux, as the former Chair of the Subcommittee on National Security, we have worked with the National Security Commission on AI and trying to anticipate the opportunities that might present to heighten our ability to protect critical assets, but also there is an opportunity here for our adversaries who are not bound by democratic institutions. They are not bound by the checks and balances and the way that we in this country value personal privacy and human rights.

China has basically full-spectrum surveillance of their entire population. Russia, as well, is in that league.

How do we engage and get the most out of AI?

And we are in a competition here, right. We are in a competition. We do not want to cede this space to China.

How do we keep up with them or, you know, maintain a lead in this area and ethically do due diligence in terms of our obligation to protect privacy rights and, you know, democratic ideals?

Mr. BOUDREAUX. Thank you, Congressman, for that question.

Yes, we are in this competitive dynamic, but I think it is important that we do not let this competition allow us to lose sight of our core U.S. values and core ethical commitments. This is a key part of legitimacy of our government and the credibility of the U.S. military and our ability to operate globally.

I think ethics and the responsible deployment of military AI systems is really part of the U.S. strength. This is what allows us to work in multinational alliances with our NATO and other partners, and so, in this way, a responsible and ethical commitment to deployment is itself a type of force multiplier.

It is also, I think, what will allow the U.S. Government, including the Department of Defense and the Department of Homeland Security, to work with the technology company providers. A number of technology companies have themselves raised concerns about the responsible deployment of AI in a number of Homeland Security or international security context, and so I think it is important to ensure that the U.S. Government maintains its commitment to ethical deployment of these technologies to ensure that that partnership with technology companies will continue.

I note that the Department of Defense has stated a set of ethical principles, including the traceability, the governability, the reliability, and the equity of military AI systems, and I think there is still some work to do in the implementation of those principles, but the U.S. can be a leader in this space by showing that there's ways to deploy these types of systems ethically and responsibly.

Mr. LYNCH. I had an opportunity to read a book called "Kill Chain." It was by one of, I think, John McCain's staffers, and it talked about the need to have a human in the chain of some of these weapon systems.

Mr. Nawabi, you seem to be familiar with that.

How do we—I mean it is almost a given that countries that have less accountability for leaders, such as authoritarian regimes like Russia and China, would have greater freedom to use a system that does not have a human in that chain of decision trees that would allow the use of that weapon.

How do we protect ourselves? What countermeasures, what might we be able to adopt to face that dilemma?

Mr. Boudreaux and then Mr. Nawabi.

Mr. BOUDREAUX. Yes, thank you.

I think maintaining, as the DoD itself has stated, appropriate levels of human judgment in the development and deployment of these technologies is really crucial, that there is a human that is making a decision about the deployment of technology and that they have actually tested and evaluated the technology to ensure that it is appropriate for the specific context. And so that, in that way, there is a human that is actually accountable that can ensure that these technologies are used responsibly.

I know that there are these pressures to reduce the level of human control, right, that might help, you know, in some ways speed the ability to deploy these systems. But at what cost? And I worry about some of the risks associated with, perhaps, escalation or even proliferation of systems that operate outside of human control.

Ms. MACE. Thank you.

And will now turn to my colleague from South Carolina, Mr. Timmons, for five minutes.

Mr. TIMMONS. Thank you, Madam Chair.

First, thank you for having this hearing, and thank you all for coming and testifying.

I am 39 years old. I am a member of the last generation, members of life before technology has just transformed things. We did not have cell phones when I was little, and then we had the big bag phone that people remember, and then, obviously, the internet. I remember dial-up, and then the iPhone came out in 2007.

And just think about the time between, I would say, the early 1990's to the mid, you know, 2010 to today. I mean, it is just enormous leaps forward in technology, and I think it has caused a lot of problems. I think our society has a difficult time dealing with our increased inter-connectivity. It has really been the end of the media. The way that you purchase and pursue advertisements has really been a problem. And, while it has caused a lot of problems in our society dealing with that, I do think that it can also be the solution. And, whether it is healthcare, fighting wars, or law enforcement, these are all things that technology can help us be more efficient at.

And so, I appreciate having this hearing today to discuss law enforcement and the military's use of this type of technology.

So, I am going to start with Mr. Kenneally.

The price of—what is the name of the—I call it dog, but it is not—what is the actual name?

Mr. KENNEALLY. Yes, so the robot is called the Vision 60 by Ghost Robotics, and as soon as we sell robots to our customers, they invariably come up with their own name for them.

Mr. TIMMONS. Sure.

Mr. KENNEALLY. They develop this very amazing, really amazing relationship——

Mr. TIMMONS. And how much is it? It was——

Mr. KENNEALLY. Yes, so the robot is $165,000.

Mr. TIMMONS. Have you done the studies on how much a drug-sniffing dog or a bomb-sniffing dog costs?

Mr. KENNEALLY. I do not have that information, you know, off the top of my head, but those are also very significant investments that are made over time, and then there is always the consideration——

Mr. TIMMONS. It takes years to train, and there is a service life, and there is food and shelter and care. I mean, I have to think that it costs drastically more than that so, and you cannot really have a bomb-sniffing and a drug-sniffing dog. You have to have one or the other, and yours can do both. So that is a pretty incredible piece of technology.

And we talked earlier. The military is currently your larger customer and law enforcement to a lesser extent?

Mr. KENNEALLY. Yes, that is correct.

Mr. TIMMONS. But I would imagine that the law enforcement role has enormous potential.

Mr. KENNEALLY. Yes. There is really three main markets that we are really focused on most broadly. That would be military, you know, DoD, law enforcement and first responders, and then on the industrial side.

So, to date, you know, the majority of our business has been with DoD, but I think if you look at how the technology development typically happens, you look at GPS, the internet, touchscreen phones, it is always kind of DoD leading the charge as that initial customer, really proving out the use cases, getting the technology more mature, decreasing cost, and then it kind of goes into law enforcement, goes into industrial.

Mr. TIMMONS. Thank you for that.

Mr. KENNEALLY. So, I think we are kind of following that similar trajectory as well.

Mr. TIMMONS. Thank you.

Mr. Nawabi, the high-altitude pseudo-satellite that you showed in your video, what are the benefits of that versus a satellite? Could you talk through that?

Mr. NAWABI. Sure. Thank you, Congressman Timmons.

So, there are several key advantages to a stratospheric pseudo-satellite or high-altitude pseudo-satellite. No. 1, we are about sixty thousand or sixty-five thousand feet. You are about 20 kilometers above ground. You are above all the weather, but you are still 20 kilometers.

A LEO satellite is, roughly, hundreds of kilometers. Most of them are in the thousands of kilometers.

Mr. TIMMONS. So, Starlinks, for example, how high are Starlinks?

Mr. NAWABI. They are usually in the several hundred, nine hundred kilometers to a thousand or so. And then geosynchronous satellites are 20 thousand miles, plus.

Mr. TIMMONS. And you are allowed—you are able to provide 5G cell service?

Mr. NAWABI. Yes. We actually had two years ago, one of the flights that you saw the video on, we flew that airplane from Spaceport, New Mexico. We took off. When we got to the stratosphere—and I had an LTE payload at that time. With the LTE

payload, I was able to make a four-way Zoom HD-quality video and voice phone call through that airplane, connecting Tokyo, Japan; Silicon Valley; Spaceport, New Mexico; and D.C.

Mr. TIMMONS. What is the distance on the ground that you can be?

Mr. NAWABI. So, one HAPS can cover about a 200-kilometer diameter circle on the ground. It has both commercial applications for disaster relief, for hurricanes, for our first response. We also HAPS for communications. The main reason why we developed it was all for commercial applications using our own commercial dollars, not government funding.

Mr. TIMMONS. How much is one of those?

Mr. NAWABI. So, these are experimental for this point, and the price points are going to be competitive with cell towers for most of the globe.

Mr. TIMMONS. OK. Well, thank you so much.

Madam Chair, I yield back.

Mr. NAWABI. You are welcome.

Ms. MACE. All right. I will now recognize Congresswoman Luna for five minutes.

Mrs. LUNA. With 81,474 unaccompanied minors or single minors being encountered at the southern border this fiscal year, and one-hundred and ninety-three percent spike in human trafficking during the 2021 fiscal year, we need to ensure that our Border Patrol agents have the technology and resources needed to secure our border, as well as address the human trafficking occurring.

DNA testing and the collection of biometric data at the southern border ensures that there's a legitimate, familiar relationship between an illegal alien and the minors that they're bringing to the border. And, under the Trump Administration, ICE utilized this DNA testing at the southern border. Unfortunately, these contracts expired when President Biden took office.

My question is for you, Mr. Rawding. I recently joined a letter led by Representative Mills regarding the Biden Administration's failure to renew the familial DNA testing by CBP at the U.S.-Mexico border. In what ways has the use of biometric data coupled with DNA testing been used to address this crisis we have been currently seeing?

Mr. RAWDING. Thank you, Congresswoman.

My expertise would be more in the biometric collection with facial recognition of what is being deployed right now. I would not be able to speak to the DNA process there. I would have to defer you to CBP.

But, specifically with the application that we built and deployed across the southern border now that is being used by the 13,000 Border Patrol agents, when migrant families are encountered and those individuals are enrolled in the application, the application we built has functionality to group individuals as family units together so that the agents can keep track of them throughout the process while they are there.

Then single adult males can be adjudicated separately, and then, when they are put into the processing systems, the data integrity stays with those individuals as they move through the cycle from initial encounter, through the processing center, to detainment, to

release. So, we have closed those gaps there so that the data integrity from initial encounter stays there, and then they can build kind of models off of those different pieces to, say, from the human trafficking piece, has any individuals been seen over the course of time.

So, basically, as human traffickers, have they been encountered at the border, maybe traveled back down to Central and South America, and now we are seeing that individual, as a recidivist, that they have been encountered with multiple groups over a short period of time. And that can really help the Border Patrol agents while they are interviewing those individuals.

They have the most data with them in front of them, and they can adjudicate that and build that into their line of questioning, which, frankly, border patrol and CBP is the best in the law enforcement community to do that.

Mrs. LUNA. For the purposes of national security, is biographic only data collection or the combination of biographic and biometric data collection more effective? So, I guess in that process.

Mr. RAWDING. Thank you.

Yes, the combination of both is kind of paramount here, right. So, there is derogatory information or information that is collected that law enforcement agencies would have collected maybe on just strictly biographic, name, date of birth, and other information related to that.

But then the biometric collection piece is where you may have an unknown subject where you would like to vet that against them, and depending on how individuals are encountered, if they give a fake name, there's combinations of names, when you are in the field and trying to adjudicate those individuals rapidly, it is much easier to, say, to utilize a face to vet against information that you have in your law enforcement systems to, say, Ryan Rawding is a match on Ryan Rawding. We have encountered this individual before. We have seen him multiple times. He is a face match.

And then we can adjudicate the different types of maybe biographic information that I give there, but the system is able recognize that I am who I say I am, or I am not who I say that I am.

Mrs. LUNA. Perfect.

Thank you, Chairwoman. I yield my time.

Ms. MACE. All right. I will now recognize Congresswoman Greene for five minutes.

Ms. GREENE. Thank you, Madam Chair.

And thank you for coming today. I believe that technology and tools that each of you are presenting to our Committee today are useful, and they are also useful to save lives, and I think that is what we are really interested in here.

Thank you for the demonstration of the robot dog. That was really incredible, absolutely intriguing, and your video presentation is incredible as well.

I also would like to talk to you all about the risk of cyber-attacks. This is something that you know we experience not only in our government agencies, even small businesses and large coperations experience cyber-attacks, which can be concerning, especially with technology like yours. And I feel pretty confident that all of you have worked very hard to prevent things like that from happening.

Another thing that I would like to talk about today with each of you is that, as the world progresses into stages that could be going to more wars, especially given the Ukraine and Russian war that is happening right now. I would like to ask each of you how we can make sure that we prevent any types of technologies or robotics like this to ever be used as weapons against people, and I think that is extremely important.

Again, it is not weaponizing technology we want to see happen ever, and I would like to see countries around the world make agreements to this, especially on emerging incredible inventions. We do not want to see them turned into something that would kill people.

But I will start with Mr. Rawding, and I will walk all the way down. Let us talk about cyber-attacks. How can we—have you—what steps can be taken to prevent cyber-attacks?

Mr. RAWDING. Thank you, Congresswoman.

I will speak specifically to the application that we have built being utilized by CBP. Our processes adheres to all DHS and CBP privacy policy. So, as they are building applications within the network, all the security protocols are in place to protect the government cell phones that the agents have and then the software that there lies within them.

Specific to some of the applications that we have deployed is we do not retain any of that information on the devices once the initial encounter has occurred and they have been pushed——

Ms. GREENE. And just to be mindful of everybody's time.

Mr. RAWDING [continuing]. Through the processing system.

So, we have set up those protocols in place to protect the devices and the application that we have built.

Ms. GREENE. OK, thank you.

Mr. Nawabi.

Mr. NAWABI. Thank you, Congresswoman.

In terms of cyber-attacks, one of the things that we pride ourselves—we have been in this business for several decades, as you know, and we have supplied the U.S. Government, all the branches, thousands of these systems. There has not been a single incident of misuse or a cybersecurity breach in our system so far. We take it very seriously. We invest a lot in it.

One of the things that actually helps us is the ability to design, manufacture, and source the entire systems in the United States, and having it actually developed internally and not use open-source algorithms or codes and software dramatically changes that paradigm and actually helps us protect it.

And that is one of the things that we invested in many years ago, and we continue to do that. That makes us far better at this than many consumer-type products that are much less expensive, but they have a lot of consequences and unintended concerns with it.

Ms. GREENE. Well done. Thank you.

Mr. Kenneally?

Mr. KENNEALLY. Yes, thank you for that question.

So, the robot, the way we built it, effectively, it is a server or a computer on legs, and so we are able to use standard best practices to lock down the robot as much as possible using fire walls. And then because of the sensitive nature of our customers, we actually

have all of the data that the robot collects is only stored locally. So, it is a very much lockdown system.

And then, to be extra safe, we have actually hired an independent firm to do pen testing, and they were not able to get into our system. So, that is something we take very seriously as well.

Ms. GREENE. OK.

Mr. Boudreaux.

Mr. BOUDREAUX. I agree that the risk of cyber-attacks are significant, and that is why it is important to have good protections with respect to what type of data is being collected by these different surveillance systems and safeguards that are implemented, such as some of the ones described. But, also, the government could play a role in instituting some of these safeguards throughout the technology acquisition and deployment process.

Thank you.

Ms. GREENE. OK, thank you.

And times up. Thank you, Madam Chair.

Ms. MACE. Yes. I apologize.

I would now like to recognize Mr. Langworthy for five minutes.

Mr. LANGWORTHY. Thank you, Madam Chair.

And I would like to thank all of our witnesses for being here today and extend a gratitude for your role that you all contribute to our Nation's border security.

We spent a lot of time talking about the southern border, and very rightfully so, but I want to spend a little time talking about our northern border today.

New York's 23d District borders Canada on Lake Erie and is roughly a 20-minute drive from the Peace Bridge in Buffalo that connects to Fort Erie. It is one of the most trafficked ports of entry on our northern border.

And, furthermore, across New York, we have a border that is experiencing an almost eight-hundred percent increase in illegal immigration in the Swanson Sector alone.

Mr. Nawabi, our northern border often reaches below zero temperatures and at times zero visibility, with high winds and heavy snow. Just this past winter, reports of families freezing to death crossing the northern border stole some headlines.

Do you believe that unmanned aerial systems technology could be effective in these conditions on the northern border and, if so, how so?

Mr. NAWABI. Thank you, Congressman Langworthy. The short answer is yes. The Puma system that you see on my right, that is actually designed to be all-environment. So, it could fly—it has flown in Antarctica and the North Pole area and Alaska. It is flying currently in places like Ukraine, the Middle East, pretty much every continent around the world.

And so, the systems that we design, one of the things that is really unique about it is it is made for the type of environments and applications that our customers require us, primarily the U.S. military and our allies.

And they need to work in very high temperatures, very low temperatures. They have got to be able to work in storms. That has to have, you know, sensors that can operate in those conditions as well.

So, A, the short answer is yes, they do make a big difference. And we invest quite a lot of R&D dollars, our own internal R&D dollars to make sure that our systems are capable of operating in those environments.

Mr. LANGWORTHY. Thank you.

Mr. Kenneally, under these same conditions, could robotics technology be used on the northern border?

Mr. KENNEALLY. Yes, absolutely. Thank you for that question. So, we also have built these robots very purposefully to go in environments that are incredibly harsh and hard for humans to traverse. So, we are able to operate the robot down to minus forty Celsius or minus forty Fahrenheit—it is the same thing—and then as well as it is fully sealed, so it can operate in all kinds of different weather conditions.

We have also operated the robots; it can actually walk in up to two feet of snow. So, we developed systems such that, even if the sensors are blocked by walking through a significant amount of snow, the robot's able to continue to make progress.

We have done testing in snow. We have done testing on ice. We actually have special treads that we have developed for the robots for traversing ice as well. So, it can actually not only walk, but it can run on sheet ice.

So, we have done a lot of that kind of development. And I think those are—there are many applications where you can work in those very harsh environments and then do, you know, either linear inspection of rail or other infrastructure or vehicle inspection with the appropriate additional sensors at the border. So, absolutely, yes.

Mr. LANGWORTHY. Thank you.

And now I know both of your technologies need human operation, but could you see your technology having life-saving impacts on not only individuals crossing the border illegally in these conditions but also for Border Patrol agents who may be in a situation where they have to risk their lives in these conditions?

Mr. KENNEALLY. Yes. I think—I mean, basically, the robots are able to collect more data and really provide more situational awareness. So, it is really our belief that more data is just going to shed light on the situation and then help us understand what risks may or may not be there and eventually save lives.

Mr. NAWABI. Thank you, Congressman. And, yes, the U.S. Customs and Border Patrol has been our customer. They currently utilize our Puma systems. And there are lots and lots of very strong use cases and applications for using technologies such as ground robots in combination with air robots, or aerial UAVs, to do border security, to perform it better, cheaper, and much more reliably as well.

Mr. LANGWORTHY. Excellent. I am sure both of you have very up-to-date technology, but I know innovation does not stop once you have the product.

Given the rapid rate at which technology advances and the slow speed in which the Federal Government works, do you fear that the government is not acquiring the most up-to-date technology?

Mr. NAWABI. Congressman, that is a pretty broad question. I can share with you our experience. I do believe that the rate of innova-

tion in technologies are very much faster than the rate that the U.S. Government, in general, acquires it and enables themselves with the capability.

Probably this Committee could do quite a bit to help in removing some of the challenges related to the acquisition process. Really, they are to some extent constrained, "they" meaning the agencies that need these systems, both in terms of funding but also in terms of the speed of the process by which they are able to acquire and get those capabilities into their hands, of the users.

Mr. LANGWORTHY. Thank you very much for your testimony.

And I yield back, Madam Chair.

Ms. MACE. All right. Thank you.

And I will now yield to Mr. Burlison for five minutes.

Mr. BURLISON. Thank you, Madam Chair. I am sorry I did not get to see the awesome demo, but I can only imagine what you were demonstrating.

But my first question is for you, Mr. Nawabi: Are the cartels using drones or any technology? Are you aware of their activity on the southern border?

Mr. NAWABI. Congressman Burlison, thank you for that question. I am personally not aware of specific cases, although I do know, in general, that much more primitive, and simpler drone technology has been reported to be used by drug cartels.

The technology that we have is far more advanced in its capability, and, to my knowledge, until—since we have been in business, it has not been in the hands of the cartels.

Mr. BURLISON. Do they ever attack our drones?

Mr. NAWABI. Not to my knowledge, Congressman.

Mr. BURLISON. OK. Mr. Kenneally, is that right? I am sorry.

Mr. KENNEALLY. Yes, it is.

Mr. BURLISON. OK, good, I got it.

My question for you is: A few House Democrat Members reportedly wrote to the U.S. Customs and Border Protection last year expressing concerns about that robotic dogs could pose a lethal threat to migrants and Americans.

How legitimate is that concern?

Mr. KENNEALLY. So, the use case where, as I mentioned, we did some testing with Customs and Border Patrol, the use case for the robots at the border is really to collect data.

So, it is—as I mentioned, you can either look for illegal drug trafficking by adding appropriate sensors to detect for that, or you can have thermal or infrared cameras on the system which will let you pick up, you know, humans or other animals, right, using those thermal signatures.

And so, the robot is really a detection system which will then actually be used to save lives, right? There are hundreds of deaths every year from people drowning or getting stuck trying to cross the border. And, so, more information along those lines I think can only be beneficial.

Mr. BURLISON. Thank you for correcting the record on that.

This is a question for each one of you on the panel. You know, regulation stymies innovation. In your business or in your process of development, have you experienced any regulations that you

could tell us about that—that stymie your innovation? And we'll just begin with Mr. Rawding.

Mr. RAWDING. Thank you, Congressman. In my experience, our experience as a company for some of the applications that we've developed and targeting systems for U.S. Customs and Border Protection, we're on a current contract. I think CBP has done really well with having multiple different contracts that kind of cover agile frameworks and deployment of software solutions. And that gives them the ability for us to come up with a concept to design and deploy something very effective to the frontline operators when they need it rather than the stovepipes of some other potential procurement processes.

Mr. BURLISON. So, you are saying the current setup works; there is no regulation that has been stymieing you.

Mr. RAWDING. In the way that we are operating now for CBP under the current pace, I would say that is correct.

Mr. BURLISON. OK. Thank you.

Mr. NAWABI. Congressman Burlison, yes, we have experienced several regulatory requirements and hurdles. One that comes to mind right now that could actually benefit from hopefully your support is the Federal Aviation Administration because the deployment and adoption of drones really requires its integration with the airspace, the national airspace.

The UAV that you saw that flew in the stratosphere, we are actively now pursuing the certification of that UAV, similar to a commercial airliner, but it is a very different airplane. There is no humans in it. There is no fuel on board. There is batteries and solar cells and electric motors.

So that is an area that the United States—and we are actually way ahead of our adversaries. And making that easier and going faster would help. Similar to the drone on my left, Quantix, was initially developed for the agriculture industry. You can do inspections of power lines, utilities, railroads.

Mr. BURLISON. Bridge, under——

Mr. NAWABI. Bridges, all sorts of infrastructure in agriculture. But you cannot today fly this unless you are in a specific test market beyond visual line of sight. So, if you cannot see the drone, then you cannot fly it.

And a lot of these applications require these drones to safely—and the technology exists for them to operate beyond visual line of sight. And that is another area that, again, FAA is involved, and they should be, but helping the regulations to address the current technology advancement and the pace by which the technology is advancing is really critical, and to not only help us as a country, but to allow us to stay ahead of our adversaries and to enable our, you know, domestic law enforcement agencies to be able to use these effectively as well.

Mr. BURLISON. Thank you.

Ms. MACE. In closing, I want to thank you all this afternoon. I thank our panelists once again for their testimony today.

Recent developments in AI will change the way we live and work, and we must maintain our edge over China in AI development. The capabilities of robots, drones, scanners and other secu-

rity hardware may be supercharged by advances in AI, and we have seen some of those advances today.

We can help ensure the most effective, newest security technologies the private sector develops gets into the hands of our Border Patrol and other Federal agencies to keep our people, our citizens, and our Nation safe.

So, I want to thank all our witnesses today—Mr. Rawding, Mr. Nawabi, Mr. Kenneally and Mr. Boudreaux—for your testimony today.

With that, and without objection, all Members will have five legislative days within which to submit materials and to submit additional written questions for our witnesses, which will then be forwarded to the witnesses for their response. So, if there is no further business today, without objection, our Subcommittee stands adjourned.

Thank you.

[Whereupon, at 2:59 p.m., the Subcommittee was adjourned.]