SMART INVESTMENTS: TECHNOLOGY'S ROLE IN A MULTI-LAYERED BORDER SECURITY STRATEGY

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON BORDER SECURITY AND ENFORCEMENT

AND THE

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND ACCOUNTABILITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

JULY 9, 2024

Serial No. 118–75

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

59–681 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*
NATALIE NIXON, *Chief Clerk*

SUBCOMMITTEE ON BORDER SECURITY AND ENFORCEMENT

CLAY HIGGINS, Louisiana, *Chairman*

MICHAEL GUEST, Mississippi
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
MORGAN LUTTRELL, Texas
JOSH BRECHEEN, Oklahoma
MARK E. GREEN, MD, Tennessee *(ex officio)*

J. LUIS CORREA, California, *Ranking Member*
SHRI THANEDAR, Michigan
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
BENNIE G. THOMPSON, Mississippi *(ex officio)*

NATASHA EBY, *Subcommittee Staff Director*
BRIEANA MARTICORENA, *Minority Subcommittee Staff Director*

SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND ACCOUNTABILITY

DAN BISHOP, North Carolina, *Chairman*

MARJORIE TAYLOR GREENE, Georgia
MIKE EZELL, Mississippi
DALE W. STRONG, Alabama
ELIJAH CRANE, Arizona
MARK E. GREEN, MD, Tennessee *(ex officio)*

GLENN IVEY, Maryland, *Ranking Member*
SHRI THANEDAR, Michigan
DELIA C. RAMIREZ, Illinois
YVETTE D. CLARKE, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*

SANG YI, *Subcommittee Staff Director*
LISA CANINI, *Minority Subcommittee Staff Director*

CONTENTS

SMART INVESTMENTS: TECHNOLOGY'S ROLE IN A MULTI-LAYERED BORDER SECURITY STRATEGY

Tuesday, July 9, 2024

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON BORDER SECURITY AND ENFORCEMENT, AND THE
SUBCOMMITTEE ON OVERSIGHT, INVESTIGATIONS, AND ACCOUNTABILITY,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:15 p.m., in room 310, Cannon House Office Building, Hon. Clay Higgins (Chairman of the subcommittee) presiding.

Present: Representatives Higgins, Bishop, Greene, Ezell, Strong, Crane, Correa, Ivey, Thanedar, Ramirez, and Clarke.

Mr. HIGGINS. This Committee on Homeland Security, Subcommittee on Border Security and Enforcement, and the Subcommittee on Oversight, Investigations, and Accountability will come to order.

Without objection, the Chair is authorized to declare the committee in recess at any point.

The purpose of this hearing is to examine the importance of emerging technologies for border security detection and inspection purposes and explore the coordination and collaboration of the Department of Homeland Security with private industry. I now recognize myself for an opening statement.

Good afternoon and welcome to the Subcommittee on Border Security and Enforcement and the Subcommittee on Oversight, Investigations, and Accountability. It's a joint hearing on technology's role in enhancing our border security.

The crisis at our Southern Border poses an existential risk to our Nation. To combat this threat, emerging border security technologies play a critical role in deterring criminal activity in the mass illegal immigration that we have witnessed under the Biden administration.

Illegal immigration has surged to an unprecedented level, with approximately 9.7 million illegal aliens crossing our border since President Biden took office. This is more than double the entire population in my home State of Louisiana.

Influx of fentanyl and other deadly drugs is destroying American families and communities. The latest data shows that in the past year, approximately 13,000 pounds of fentanyl had been seized at the Southwest Border. Cutting-edge technology is crucial in interdicting these dangerous substances and apprehending drug traffickers.

Furthermore, dangerous cartels continually exploit vulnerabilities in our border security. DHS's partnership with the private sector is crucial in leveraging the most advanced technologies available to identify, track, and respond to these threats on land, air, and sea. We have a responsibility to our Nation to use every tool and technology at our disposal to protect our homeland from these threats.

DHS's deployment of emerging technologies is necessary to combat the illegal movement of aliens, drugs, weapons, and other illicit commodities from crossing the United States border. As transnational criminal organizations and terrorists constantly seek new methods to penetrate the vulnerable border, these innovative technologies are essential in countering the evolving threat, including the use of cartel drones and coyote-smuggling operations.

The commercial security industry has always played a vital role in protecting America's homeland. Private-sector investments in new technologies have enabled components such as Customs and Border Protection to properly and strategically deploy personnel and technology to maximize the agency's effectiveness and fulfill its mission.

I'd like to express my gratitude to our witnesses for appearing before the committee today and to discuss how DHS works with industry to provide advanced solutions to our law enforcement personnel on the ground, emblematic of the many private partners working with DHS to secure our homeland.

Border security technology will never replace front-line agents and officers. However, technology can be a critical tool to aid law enforcement personnel to carry out their mission. The need for advanced technology will continue to grow, as well as the need for personal investment from each one of us as Americans, for us as a committee to support, to prepare the necessary agents on the ground to defend our Nation.

With that, I yield back the balance of my time. I look forward to hearing from the witnesses.

[The statement of Chairman Higgins follows:]

STATEMENT OF CHAIRMAN CLAY HIGGINS

JULY 9, 2024

Good afternoon and welcome to the Subcommittee on Border Security and Enforcement and the Subcommittee on Oversight, Investigations, and Accountability joint hearing on technology's role in enhancing our border security.

The crisis at our Southern Border poses an existential risk to our Nation. To combat this threat, emerging border security technologies play a critical role in deterring criminal activity and the mass illegal immigration that we have witnessed under the Biden administration.

Illegal immigration has surged to an unprecedented level with approximately 9.7 million illegal aliens who have crossed our borders since President Biden took office. This is more than double the entire population of my home State of Louisiana.

The influx of fentanyl and other deadly drugs is destroying American families and communities. The latest data shows that in the past year, approximately 13,000 pounds of fentanyl have been seized at the Southwest Border. Cutting-edge technology is crucial in interdicting these dangerous substances and apprehending drug traffickers.

Furthermore, dangerous cartels continually exploit vulnerabilities in our border security. DHS's partnership with the private sector is crucial in leveraging the most advanced technologies available to identify, track, and respond to these threats on land, air, and sea.

We have a responsibility to our Nation to use every tool and technology at our disposal to protect our homeland from these threats.

DHS's deployment of emerging technologies is necessary to combat the illegal movement of aliens, drugs, weapons, and other illicit commodities from crossing the United States Border.

As transnational criminal organizations and terrorists constantly seek new methods to penetrate the vulnerable border, these innovative technologies are essential in countering these evolving threats, including the use of cartel drones and coyote smuggling operations.

The commercial security industry has always played a vital role in protecting America's homeland. Private-sector investments in new technologies have enabled components such as Customs and Border Protection (CBP) to strategically deploy personnel and technology to maximize the agency's effectiveness and fulfill its mission.

I would like to express my gratitude to our witnesses for appearing before the committee today to discuss how DHS works with industry to provide advanced solutions to our law enforcement personnel on the ground, emblematic of the many private partners working with DHS to secure our homeland.

Border security technology will never replace front-line agents and officers. However, technology can be a critical tool to aid law enforcement personnel carry out their mission. The need for advanced technology will continue to grow, as well as the need for personnel ready to defend our Nation.

With that, I yield back the balance of my time and look forward to hearing from our witnesses.

Mr. HIGGINS. I recognize the Ranking Member, my friend, Mr. Correa, to speak his opening statement.

Mr. CORREA. Thank you, my good friend, Chairman Higgins. Thank you, Chairman Bishop, for holding this important hearing, and, of course, welcome to our witnesses today. Do hope to learn more about what Congress can do to do a better job preparing, implementing the latest technologies at our borders.

Today presents an opportunity to hear about the new technologies that can support homeland security. I hope that we in Congress learn the lessons that you all too well know to continue to protect the homeland. I'm pleased to see the Biden administration prioritize integrating advanced technologies like AI, or artificial intelligence, into homeland security initiatives, while still ensuring the protection of civil rights and civil liberties. Advanced technologies will help CBP officers and agents work more efficiently and effectively to keep the American people safe.

I must say that our Nation has always been a Nation of international trade and commerce. My home State, California, the San Ysidro-San Diego border crossing every day over 70,000 vehicles cross and over 20,000 pedestrian cross that border on a daily basis.

Our border customs officers, those folks in the blue uniforms, scanned vehicles using AI-powered machines to detect and interdict drugs and other dangerous substances before they enter our country. These systems not only allow for better targeting, but also for quicker inspections. Facilitating the timely flow of trade and travel helps keep the economy strong.

Last year Nation-wide, CBP used over 370 nonintrusive inspection scanners to examine more than 9 million conveyances, resulting in the seizure of more than 127,000 pounds of narcotics and the identification of 125 undeclared passengers. But, clearly, the challenge—the scale of the challenge is huge, and more technology is needed.

More scanners means less fentanyl on our streets. More investment in cameras in ground-based sensors means more data that our officers and agents can use to stop human smugglers and human traffickers.

But as all of you know, technology isn't enough. In fact, it's the well-trained men and women at our border that are our greatest resource, and technology helps them do a good job. But the women, men—men and women at our front lines are very critical.

Sadly, our ports of entry today need over 5,000 more CBP officers. Five thousand more CBP officers are needed at our border today to do the job we are asking them to do. Border Patrol is also facing a major shortfall. Even the best technology cannot fill these gaps, and we should also remember that border security does not start or end at our border.

Excuse me for a minute. We need the cooperation of our neighbors across the hemisphere to tackle the big problems. We need to be working with Mexico to counter drones and go after smugglers and traffickers. We need to be working with the South American countries to screen passengers coming into the hemisphere at the point of origin. We need to I.D. potentially dangerous individuals before they even get on a plane to come to this hemisphere.

Lot of cooperation is happening, but it's still not enough. Back home in California, we look at the border as an economic driver that adds to our economic growth. California today is the fourth-largest economy in the world. Trade and travel across our borders boosts our economic output and brings us closer to our southern neighbors.

Today, as Members of Congress, we support ways to increase legitimate trade and travel while keeping the American public safe. We often use technology to do this, but, sadly, the timely and cost-effective deployment of technologies has been a long-standing challenge for CBP. It is vital that the Federal Government collaborate with the private sector to develop and adopt cost-effective and innovative technologies sooner rather than later.

To help address this problem, I've worked with Congressman Luttrell to introduce the Emerging Innovative Border Technologies Act, and this bill addresses the capability gaps at border security by requiring the Secretary of Homeland Security to submit a plan to Congress to identify, integrate, and deploy innovating technologies, like AI, machine learning, and nanotechnology into our border security initiatives. This is just one of many other things Congress can be doing to help the men and women at the border.

I look forward to hearing your recommendations today, gentlemen. You are the experts. Let us know what else we can do to make sure that technology comes to the forefront of our battles at the border immediately, not 5, 10, 20 years later.

Thank you very much. Mr. Chairman, I yield.

[The statement of Ranking Member Correa follows:]

STATEMENT OF RANKING MEMBER J. LUIS CORREA

JULY 9, 2024

Today presents an opportunity to hear about innovative technologies that can support and strengthen the Department of Homeland Security's border security effort. I hope we also learn how Congress can do more to ensure our front-line personnel have access to the technology they need when they need it.

I've been pleased to see the Biden administration prioritize integrating advanced technologies like artificial intelligence into homeland security initiatives, while still ensuring the protection of civil rights and civil liberties.

As I am sure we will hear more today, advanced technologies can help CBP officers and agents work more efficiently and effectively to keep the American people safe. At San Ysidro in San Diego alone, over 70,000 vehicles and 20,000 pedestrians enter the United States every day. There, our Customs officers—the blue uniforms—scan vehicles using AI-powered machines to detect and interdict drugs and other dangerous substances before they enter our communities. These systems not only allow for better targeting, but also for quicker inspections than intrusive manual inspections. Facilitating the timely flow of trade and travel helps keep our economy strong.

Looking Nation-wide, last year CBP used over 370 non-intrusive inspection scanners to examine 9.2 million conveyances, resulting in the seizure of more than 127,000 pounds of narcotics and the identification of 124 undeclared passengers. The scale of the challenge is clearly immense.

More technology is needed. More scanners mean less fentanyl on the street. More investments in cameras and ground-based sensors means more data that our officers and agents can use to stop human smugglers and human traffickers.

But technology isn't enough. In fact, well-trained personnel are still the Department's greatest resource. Technology helps them do their jobs, but the men and women on our front lines who staff our ports of entry and work between ports of entry are absolutely critical. Unfortunately, our ports of entry need over 5,000 more CBP officers to do all of the work ask them to do. Border Patrol is also facing a shortfall. Even the best technology cannot fill these gaps.

We should also remember that border security does not start or end at our border. America alone cannot solve our border security challenges. The right technology and personnel can help, but we need cooperation across our hemisphere to tackle the big problems. We need to be working with Mexico to counter drones and go after smugglers and traffickers.

We need to be working with South American countries to screen flights arriving in the hemisphere for individuals, particularly dangerous individuals, who may attempt to cross unlawfully into the United States. A lot of cooperation is happening already. But we still need more. Our foreign partnerships are vital to securing our border.

In my State, we see the border as more than a national security issue. It's the economic driver for my community and many others. Trade and travel across the border support our economy—the greatest thing we have as a country to compete with other countries. It boosts our economic output and bring us closer with our southern neighbors. As Members of Congress, we support ways to power the growth of legitimate trade and travel while still keeping American communities safe.

We often use technology to do this. But unfortunately, the timely and cost-effective deployment of technologies has been a long-standing issue for CBP. It is vital that the Federal Government to collaborate with the private sector and venture capital to develop and adopt cost-effective and innovative technologies.

To help address these problems, I worked with Congressman Luttrell to introduce the Emerging Innovative Border Technologies Act. This bill addresses capability gaps in border security operations by requiring the Secretary of Homeland Security to submit a plan to Congress to identify, integrate, and deploy innovative technologies like AI, machine learning, and nanotechnology into border security initiatives.

This is just one of likely many things that Congress could do to help our men and women at the border. We must continue to work together to create opportunities for CBP to utilize innovative technologies to protect national security and facilitate trade and travel at the Southern Border. I look forward to the recommendations from our witnesses.

Mr. HIGGINS. The Ranking Member yields. I now recognize the Chairman of the Subcommittee on Oversight, Investigations, and

Accountability, the gentleman from North Carolina, Mr. Bishop, for his opening statement.

Mr. BISHOP. Thank you, Mr. Chairman. Good afternoon to everyone attending. Thank you to our witnesses for joining us today to share your insights on how the Department of Homeland Security can partner with the private sector for technological solutions to enhance border security.

As Chairman of the Subcommittee on Oversight, Investigations, and Accountability, I have no doubt of the critical need for DHS to take advantage of technology to increase the operational effectiveness of the agents responsible for securing our Nation's borders. The new technologies act is a force multiplier for CBP agents in the field and providing them with greater situational awareness and enabling more efficient use of CBP resources.

For example, the deployment of autonomous surveillance towers, unmanned aerial systems, and other surveillance technology along the border facilitates real-time monitoring for potential threats, especially in remote areas that are far more difficult for Border Patrol agents to cover.

We know that there have been more than 1.8 million got-aways at the border since January 2021, 194,000 since October 2023. That's a major national security crisis. Using technology to detect and prevent these threats must be a critical priority.

In a 2021 report, however, the DHS inspector general found that CBP lacks sufficient personnel to fully leverage surveillance technology advances. Using artificial intelligence can help alleviate the manpower issue. Enabling surveillance and processing tools to operate with greater autonomy may reserve time for agents to attend to the most significant threats personally. Automating previously labor-intensive tasks also helps free Border Patrol agents to get back in the field to safeguard the homeland.

Similarly, using—the use of nonintrusive screening equipment and facial recognition technology at land ports of entry plays a critical role in protecting the homeland while facilitating lawful trade and travel. Our recent inspector general report also found that, because of limitations in camera technology, CBP had only a 76 percent success rate in capturing images of vehicle passengers at ports of entry, and of those captured, only 81 percent were of sufficient quality to conduct adequate screenings.

Staying at the cutting edge of technology is vital to national security and defending our border, particularly as cartel tactics and use of technology have become increasingly advanced. In recent years we've seen cartels routinely deploy sophisticated and widely available drones to conduct countersurveillance on Border Patrol and to advance their smuggling operations.

In February last year, Chief Sector Patrol Agent Chavez testified that the Rio Grande Valley sector had experienced over 10,000 drone incursions in a single year. It is not hard to imagine that cartels have increased the frequency of incursions since then.

In transcribed interviews with the committee, multiple sector chiefs affirmed that cartels seek to exploit any perceived vulnerabilities to facilitate human and drug smuggling across the border between ports of entry. CBP's adoption and implementation of advanced C–UAS technology is crucial to denying cartels the ability to freely operate drones across the border.

The House Majority emphasized the importance of border technology when it passed the border security bill, H.R. 2, requiring CBP to present a 5-year strategic technology investment plan that lists security technology priorities needed to address risks and capability gaps. The bill also requires CBP to provide clear goals and time lines for implementing their technology priorities.

H.R. 2 also requires CBP to take steps to streamline the acquisition process and increase partnerships in consultation with the private sector to ensure that CBP is well-informed on technological advances and innovations relevant to the border security mission. The CBP innovation team has legislative authority to fast-track technology projects up to $25 million.

As CBP considers and pilots new technologies, it is important to define success and identify performance metrics to ensure that money is spent efficiently and effectively. According to the Government Accountability Office, as of July 2022, the CBP innovation team invested more than $120 million in 73 cutting-edge technology pilot projects. At the time of the report, however, the team had not clearly derived strategic-level goals or quantified performance goals to assess progress.

In an environment as fast-paced and crucial to homeland security as the Southern Border, it is imperative to identify metrics for success in implementing new technologies. It is my hope that our witnesses can help identify these metrics and performance goals so Congress can conduct meaningful oversight over CBP's technology investments.

Of course, technology can't replace the need for Border Patrol agents, a border wall, and the basic will to enforce our immigration laws. It is not a silver bullet to solve the border crisis, but it can help the men and women of Border Patrol to be more effective in carrying out their mission of securing America's borders.

Today's hearing is about how DHS can work with the private sector to deliver smarter security and ensure that taxpayer dollars are being used for the greatest effect. I look forward to an informative hearing with our witnesses.

I yield back.

[The statement of Chairman Bishop follows:]

STATEMENT OF CHAIRMAN DAN BISHOP

JULY 9, 2024

Good afternoon and thank you to our witnesses for joining us today to share insights on how the Department of Homeland Security can partner with the private sector for technological solutions to enhance border security.

As Chairman of the Subcommittee on Oversight, Investigations, and Accountability, I have no doubt of the critical need for DHS to take advantage of technologies to increase the operational effectiveness of the agents responsible for securing our Nation's borders.

These technologies act as a force multiplier for CBP agents in the field, providing them with greater situational awareness and enabling more efficient use of CBP resources.

For example, the deployment of autonomous surveillance towers, unmanned aerial systems, and other surveillance technology along the border facilitates real-time monitoring for potential threats, especially in remote areas that are more difficult for Border Patrol agents to cover.

We know that there have been more than 1.8 million gotaways at the border since January 2021, including 194,000 since October, 2023. That's a major national security crisis. Using technology to detect and prevent these threats must be a critical priority.

In a 2021 report, however, the DHS inspector general found that CBP lacked sufficient personnel to fully leverage surveillance technology advances.

Using artificial intelligence can help alleviate the manpower issue. Enabling surveillance and processing tools to operate with greater autonomy can reserve time for agents to review the most imminent threats. Automating previously labor-intensive tasks also helps free Border Patrol agents to be back out in the field to safeguard the homeland.

Similarly, the use of non-intrusive screening equipment and facial recognition technology at land ports of entry plays a critical role in protecting the homeland while facilitating lawful trade and travel.

A recent inspector general report also found that because of limitations in camera technology, CBP had only a 76 percent success rate in capturing images of vehicle passengers at ports of entry. And, those captured, only 81 percent were of sufficient quality to conduct adequate screenings.

Staying on the cutting edge of technology is vital to national security and defending our border, particularly as cartel tactics and use of technology have become increasingly advanced.

In recent years, we've seen cartels routinely deploy sophisticated and widely available drones to conduct countersurveillance on Border Patrol to advance their smuggling operations.

In February of last year, Chief Sector Patrol Agent Chavez testified that the Rio Grande Valley sector had experienced over 10,000 drone incursions in a single year. It is not hard to imagine that cartels have increased the frequency of incursions since then.

In transcribed interviews with the committee, multiple sector chiefs affirmed that cartels seek to exploit any perceived vulnerabilities to facilitate human and drug smuggling across the border between ports of entry. CBP's adoption and implementation of advanced C–UAS technology is crucial to denying cartels the ability to freely operate drones across the border.

The House Majority emphasized the importance of border technology when it passed the border security bill, H.R. 2, requiring CBP to present a 5-year strategic technology investment plan that lists security technology priorities needed to address risks and capability gaps. The bill also requires CBP to provide clear goals and time lines for implementing their technology priorities.

H.R. 2, also requires CBP to take steps to streamline the acquisition process and increase partnerships and consultation with the private sector to ensure that CBP is well-informed on technological advances and innovations relevant to the border security mission.

The CBP Innovation Team has legislative authority to fast-track technology projects up to $25 million dollars. As CBP considers and pilots new technologies, it is important to define success and identify performance metrics to ensure that money is spent efficiently and effectively.

According to the Government Accountability Office, as of July 2022, the CBP Innovation Team invested more than $120 million in 73 cutting-edge technology pilot projects. At the time of the report, however, the team had not clearly derived strategic-level goals or quantified performance goals to assess progress.

In an environment as fast-paced and crucial to homeland security as the Southern Border, it is imperative to identify metrics for success in implementing new technologies. It is my hope that our witnesses can help identify these metrics and performance goals so Congress can conduct meaningful oversight over CBP's technology investments.

Of course, technology can't replace the need for Border Patrol agents, a border wall, and the basic will to enforce our immigration laws. It's not a silver bullet to solve the border crisis, but it can help the men and women of Border Patrol to be more effective in carrying out their mission of securing America's borders.

Today's hearing is about how DHS can work with the private sector to deliver smarter security and ensure that taxpayer dollars are being used for the greatest effect. I look forward to an informative hearing with our witnesses.

Mr. HIGGINS. Thank you, Chairman Bishop.

I now recognize the Ranking Member of the Subcommittee on Oversight, Investigations, and Accountability, the gentleman from Maryland, Mr. Ivey, for his opening statement.

Mr. IVEY. Thank you, Chairman Higgins, Chairman Bishop, Ranking Member Correa. To the witnesses, thank you for appearing today. I look forward to your testimony.

I think my colleagues have raised a lot of the points that I wanted to touch on. But with respect to the technology piece for detecting, whether it's contraband coming across the border or drones, I think it's critical that we make some immediate and aggressive steps to try and address that.

We've got—when I had a chance to go down to the Rio Grande Valley—it was about a year ago, I guess—we had a chance to see some of the technology that was at work. This picture to my right shows one of the scanners that's used for trucks as they come through. You can see the result on my left side.

So it's almost like an X-ray or an MRI machine that can detect what's going on inside the truck, and it's been very effective, as I understand it, at identifying contraband and slowing the flow.

You can put them down.

The challenge at the time was they didn't have enough of them for the ports of entry. I know that they've been trying to expand that number over time.

One of the things I'd like to hear about today is where we are on that process, because they had the ability to transmit back to a central location the results from each one of those, just like if you went to get an X-ray at your radiologist, the radiologist might not be reading it at the place where the X-ray is being done. They might be at a different location. That allows a more efficient use of the technology. It also allows more use of AI, because AI does a better job of scanning than the human eye does.

So one of the things I'd like to hear about is to what extent we've integrated the AI into this process and how extensively we're using these. Because I was told at the time—and, again, that was almost a year ago, which is like dog years in tech. That's, like, 20 years almost. But, you know, how far have we come on that front?

Because if it's that effective—and I think everybody agrees that—and Border Patrol was certainly in support of it—let's see if we can expand it and do more with it to intercept more. Because everybody agrees that fentanyl and other contraband coming across the border has been devastating to the country.

If we can have these kinds of solutions, which aren't super expensive—they're not cheap, but they're, you know, worth the weight of the—worth their weight in gold, I would say—we should be trying to move in that direction quickly.

As the point was made a few minutes ago, yes, we need Border Patrol agents. When we were down there, they said they needed assistance. We've heard at hearings and some of the reports we've gotten back from Homeland that they're 5,000 short on officers and agents. I know we're taking other steps to try and address that.

We're working our way through the appropriations process, and there's some hang-ups there that we need to work through, I think, to make sure that there are no cuts to Homeland or—I think the White House budget is the way to go. It's a little less than what's been proposed by House Republicans here, but I think we have to find a way to get the money to the front.

Because I think we all agree that—we might disagree about a lot of things, but I think we all agree that the resources need to go to the border to help address these kinds of issues.

I also wanted to talk a little bit about drones. My colleague, Chairman Bishop, mentioned that already. But that was another one that was brought to our attention when we were down there at the border.

They Border Patrol agents were saying that they were outnumbered 17 to 1 on drone usage and that the drones that the cartels had were more sophisticated than the ones that we had allocated to them. I'm hoping that that's changed over time, but I'm not sure.

Then, of course, the other thing that we need to pay attention to is the rapid transformation of drone technology, in part based on what's going on in Ukraine and in part what's going on in Gaza. When I was in Israel a few weeks ago, we had a chance to tour a company called Rafael that's developing anti-drone technology that is pretty amazing.

These are the guys that invented Iron Dome, the technology they've got for intercepting drones. I believe we are working—we being the United States and the Department of Defense—to get that rolled out quickly. But as you heard a few minutes ago, the cartels are using it for reconnaissance purposes, as well as smuggling purposes, and we're not giving our people at the border an equal chance to compete and fight back with that. So to the extent we can do that quickly, I think we should do it.

Now, I know there's a couple of bills that are pending in the Congress, in the House here. One of them, I think, had 3 committees it had to go through, and I know Chairman Bishop referenced H.R. 2 as well. We've got to make sure that, you know, the pieces of those bills that need to get done so we can address the drone issue, that has to happen.

I know, you guys, that's not your bailiwick there—I'm talking to the witnesses, but I'm talking to our House of Representatives, too. These are the kinds of things that we need to get done so that we can get the tools to our people who are on the border and arm them in the fight that they're waging right now.

I also wanted to mention quickly the—DHS's OTA, the Office of Transaction Authority, that does—that allows the Department to bring in cutting-edge technology that can be used on these fronts, and I know Ranking Member Correa and our colleague, Mr. Luttrell, who is not here, but—have legislation to help with this, too. We want to make sure we're moving all of this legislation forward as quickly as possible.

I know this is a Presidential election year. I know all of us are up for re-election or election to something, you know, whatever. But this is one where I think we have to find common ground and move this legislation, let—the pieces of legislation so we can enable our people at the border to defend us and give them the tools that they need to do it effectively.

With that, I yield back.

Mr. HIGGINS. Thank you, Ranking Member Ivey. Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 9, 2024

I welcome today's hearing on border security technology as I have long supported small businesses interested in partnering with the Department of Homeland Security (DHS) to fulfill the Department's essential mission of securing our Nation.

I appreciate that the Biden-Harris administration and DHS have been dedicated to increasing opportunities for small business owners as the Nation strives to fulfill America's foundational promise. President Biden is successfully carrying out his pledge to help minority-owned businesses grow by increasing the amount of Federal funds spent on contracts with small, disadvantaged businesses.

In fiscal year 2023, the Biden-Harris administration awarded an all-time high of $178.6 billion in Federal contracts to small businesses, including disadvantaged businesses. DHS obligated $9.9 billion to small businesses—the most in Department history. In contrast, Republicans are proposing significant cuts to the Small Business Administration and attempting to defund the President's agenda to advance racial and gender equity in Federal contracts. Republicans fail to recognize that when small businesses—the backbone of America's economy—engage in Government procurement, they have the potential to foster job creation, diversity, competitiveness, and innovation.

Unfortunately, the Federal procurement process may be complicated and challenging to manage, particularly for businesses that have never done business with the Government before. I look forward to hearing today how we can strengthen the ability of businesses, especially small businesses, to secure contracts with DHS to increase the use of novel technologies, including border technologies.

Technology can have a profound impact on how we secure the homeland and protect the American people. It can be a tremendous force multiplier for the officers at ports of entry and agents in the field who work tirelessly to prevent dangerous people and contraband from entering our country. Technology makes it possible to inspect more vehicles and cargo, identify who is entering the country, and detect illegal border activity. However, we must use technology in a responsible manner that protects privacy, civil rights, and civil liberties.

I also look forward to discussing today how we can ensure compliance with privacy policies and individual rights protections, such as due process and non-discrimination, as we field new and advanced border technologies.

Mr. HIGGINS. I'm pleased to welcome our panel of witnesses, and I'll ask that all witnesses please rise and raise your right hand.

[Witnesses sworn.]

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

I'd now like to formally introduce the witnesses. The Honorable Thaddeus Cleveland—this is the one time I get to call you Thaddeus—is the sheriff of Terrell County, Texas. He was appointed in 2022 and was later elected to office. Before becoming the sheriff, Cleveland had a distinguished career in the United States Border Patrol serving for over 26 years.

His last 11 years in Border Patrol was spent as a patrol agent in charge of the Sanderson Border Patrol station. Sheriff Cleveland served in multiple locations throughout Arizona, New Mexico, and Texas. He also served as an assistant chief in Washington, DC.

The gentleman seated to the sheriff's left, Mr. Carl Landrum, is the vice president of Civilian Programs and Strategy for Dedrone, a leader in smart airspace security. Dedrone employs sophisticated machine learning video algorithms to detect and pinpoint the position of drones from high-resolution video camera feeds and is used to counter malicious drones.

Prior to joining Dedrone, Mr. Landrum co-founded Landrum Strategies, LLC, a business strategy development firm, and served as the chief patrol agent of the Laredo sector of the United States Border Patrol.

He was with the Department of Homeland Security for over 27 years in various border security roles. Highly experienced gentleman.

To Mr. Landrum's left is Mr. David Berteau. The honorable David Berteau is the president and chief executive officer of the Professional Services Council. With more than 400 members, PSC is an advocate of and resource for the Federal services industry.

As CEO, Mr. Berteau focuses on legislative and regulatory issues related to Government acquisition, budgets, and requirements to improve communications between Government and industry. Prior to PSC, Mr. Berteau was confirmed in 2014 as the assistant secretary of defense for logistics and material readiness, overseeing $170 billion in Department of Defense logistics funding.

I thank the witnesses for being here today. The witnesses' full statements will appear in the record.

I now recognize Sheriff Cleveland for 5 minutes to summarize his opening statement.

STATEMENT OF THADDEUS C. CLEVELAND, SHERIFF, TERRELL COUNTY, TEXAS

Sheriff CLEVELAND. Chairman Higgins, Chairman Bishop, Ranking Members Ivey and Correa, other distinguished Members, thank you for the opportunity to be here today to talk to you about Terrell County, Texas, and our role at the Terrell County Sheriff's Office and border security efforts.

Other than my time in the United States Air Force and my time here in Washington, DC, as a Border Patrol agent assigned to U.S. Border Patrol headquarters, I have spent a lifetime on the U.S.-Mexico border as both a resident and a Border Patrol agent.

As you mentioned, I did spend 26 years in the United States Border Patrol, the last 11 years as patrol agent in charge of the Sanderson Border Patrol station, which is my home town out in Terrell County, Texas, and it's also where I am the sheriff now.

I'd still be a Border Patrol agent, but, unfortunately, we lost our sheriff to a heart attack, Santiago Gonzalez, Jr. I must say his name. He was a very good friend of mine, and he was also a 30-year veteran of the United States Border Patrol. He was our sheriff for a year, and at the age of 55 had a heart attack.

It was at that time I knew it was time for me to take care of my community in a different manner and still be able to support the United States Border Patrol. I'll be honest with you, I think I can support them more from being the sheriff than I could as patrol agent in charge.

When I talk about Terrell County, it's the tenth-largest county in the State of Texas. It's out in the Big Bend region, some of roughest, toughest, most remote border area along the entire 2,000-mile border with Mexico. Terrell County has 54 miles of river with Mexico, and it's a 2,300-square-mile county.

The U.S. Border Patrol station there has 91 miles of border. That's the third-largest amount of border by any station in the United States Border Patrol.

With that being said, at the sheriff's office, fortunately, we now have 5 of us, to include myself. Through Governor Abbott's operation, Lone Star, we've been able to hire 2 additional deputies for that 2,300 square miles. Then the U.S. Border Patrol has about 50 agents. The reason they don't have a lot of agents is we don't have the same amount of activity they do at other places along the border. However, the activity we do have there is just important.

I want to talk about activity. Like the rest of the border, we've seen a significant increase over the last 3 years—3½ years. The highest watermark we've had was a 417 percent increase in illegal alien apprehensions. Again, that's our county alone, 417 percent.

We had a 469 percent increase in got-aways. Again, that's the highest watermark. Each year over the last 3½ years, we've had significantly more apprehensions in our portion of the border. With that being said, historically, we'd have 1 death, and we've had 37 deaths over the last 3 years in our portion of the border.

Mr. Landrum and myself, both being Border Patrol agents, we've seen the evolution of technology deployments in the U.S. Border Patrol, going back from historical seismic centers in the ground that you often had to drive, you know, hours, miles to go and check to verify what actually crossed that piece of Earth, if you will, look for sign, look for footprints. We've seen that evolve to BuckEye game camera systems and other camera systems that will send us real-time images to our desktop computers.

We've also seen remote video surveillance, what we used to call scope trucks, now remote video surveillance systems that were—it used to be just a blob on the screen. Well, that technology, obviously, has also increased, and now we have almost crystal-clear pictures that we're able to observe and distinguish if it's an animal or if it's a human. That's also coupled with radar.

At my station—and, Chairman Bishop, you mentioned autonomous surveillance towers. I was the patrol agent in charge when we deployed our first 8 towers. Now we have 11, I believe, in Sanderson, and that technology is really, really beneficial because you don't have to have an agent sitting behind a desk monitoring the camera. The radar and the technology does it for the agent until it has an activation, and then it assists in tracking.

But as you all pointed out, with that type of technology, unless you have enough Border Patrol agents on the ground to go out and apprehend those that it detects, it's useless. In my environment there in Terrell County, we've experienced that quite a bit. We have what is called task saturation where our technology detects so much that we just don't have the personnel to go out and chase it.

That's where my office comes in as far as to help support U.S. Border Patrol. Look, in Terrell County, we don't have a crime problem. What we have is a border security problem.

Back in 2008, I also spent 6 months at the State of Texas border security operations center that was ran by Texas Department of Public Safety. I was Border Patrol's representative there. That is when they first deployed their drawbridge camera systems. They now have over 7,000 cameras along the U.S.-Mexico border. Those provide joint feeds to both the Border Patrol as well as the Texas Department of Public Safety.

I see my time is cutting short here. I just want to mention also that—I know we talked about multi-layered defense, and we're often talking about technology in that aspect, but I can tell you what else we need.

It's still—regardless if we're at, you know, 8 million illegal aliens crossing or 400,000, it takes partnerships. That's where, again, our office comes to play along the border, as well as Texas Department of Public Safety, Texas Parks & Wildlife game wardens, and, of course, Texas military forces.

Last comment I would just like is to acknowledge the work that U.S. Border Patrol agents do, specifically there in my home town of Sanderson, as well as the Terrell County Sheriff's Office, just a tremendous amount of work that's been done. Thank you.

[The prepared statement of Sheriff Cleveland follows:]

PREPARED STATEMENT OF THADDEUS C. CLEVELAND

JULY 9, 2024

Chairman Higgins, Chairman Bishop, Ranking Member Correa, Ranking Member Ivey, and distinguished Members of the committee, thank you for the opportunity to discuss the conditions along the Southwest Border and the efforts by the Terrell County, Texas, Sheriff's Office to serve and protect our citizens.

I am honored to represent the citizens of Terrell County and describe to you what the citizens, law enforcement, and Border Patrol experience in our portion of the United States and Mexico border.

Other than my time in the United States Air Force and in Washington, DC, while assigned to U.S. Border Patrol Headquarters, I've spent my entire life as a resident and in the U.S. Border Patrol along the U.S./Mexico border. The last 11 years of my 26-year Border Patrol career were spent as the patrol agent in charge of the Sanderson Border Patrol Station, which is also my home town and where I am Sheriff.

As background, Terrell County is located in the rugged, unforgiving, vast Big Bend Region of Texas and shares 54 miles of international border with Mexico. Terrell County is the 10th-largest county in the State of Texas and encompasses almost 2,400 square miles. The Border Patrol Station there is responsible for 91 miles of border, which is the third-largest portion of border with Mexico by a United States Border Patrol Station along the entire U.S./Mexico border.

Terrell County, does not have a crime problem, we have is a Border Security problem. Over the last 3½ years, Terrell County like much of the Southwest Border has seen a significant increase in illegal alien apprehensions; however, what has happened in Eagle Pass, Del Rio, El Paso, Lukeville, and San Diego with masses of people crossing the border, does not happen in Terrell County. What we experience are people who do not want to be apprehended nor give up. When we encounter them in the desert, they run. When we encounter them on the highways, they lead us in high-speed pursuits before bailing out and absconding.

The next set of statistics I am going to share with you are the Sanderson Border Patrol Station fiscal year apprehension and gotaway percentages compared to fiscal year 2020. In fiscal year 2021 there was a 289 percent increase in illegal alien arrests and a 323 percent increase in gotaways. In fiscal year 2022, there was a 417 percent increase in illegal alien arrests and a 467 percent increase in gotaways. Last fiscal year, there was a decrease in apprehensions and gotaways, but it was still higher than the historical numbers with 189 percent increase in illegal alien arrests and 203 percent gotaways.

Citizens of Terrell County pay the price daily for the out-of-control Southwest Border. We do not have the financial, medical, or emergency resources as many of the other larger communities affected by the activity along the border. Yet, the negative and detrimental results are the same. Valuable and costly emergency and medical resources are too often diverted to border security. In my county, landowners have to repair waterlines, fences, and structures destroyed by illegal aliens crossing their properties, as well as the significant trash, human biohazard waste, and erosion. Emergency medical services and law enforcement service has at times been unavailable due to responding to illegal aliens that are crossing the border.

There has been a total of 37 known deaths of illegal aliens attempting to cross my portion of the border over the last the 3½ years. Historically, there was 1 a year. All but 4 of those deaths were from exposure due to the hot summer months as well as the cold winter fronts that come through Terrell County. Four died in a vehicle pursuit, which resulted in a head-on collision. High-speed pursuits occur with almost every illegal alien smuggling load encountered and puts citizens my team and I are responsible for in harm's way.

Due to the amount of illegal alien smuggling activity coupled with the amount of vehicle pursuits we were involved in since I took over as Sheriff, I reached out to Governor Abbott of the State of Texas and requested additional resources to assist my office. Governor Abbott and I discussed the situation, and within a week, the additional resources I requested were allotted. With assistance from the Texas Department of Public Safety and Texas Parks and Wildlife, together we seized over 100 vehicles from illegal alien smugglers in the months of November 2022. Since then, we have observed a shift in tactics by smugglers and are not seeing the same level of activity in Terrell County. Those shifts in tactics is what brings us together today to discuss technology and advancements.

I have seen the U.S. Border Patrol evolve with technology. Technological evolutions have assisted the U.S. Border Patrol achieve tremendous success with border security. I've witnessed seismic and magnetic sensors evolve into imaging sensors, scope trucks have evolved from black blobs on a screen to Mobile Video Surveillance Systems, which use infrared night vision and radars with a near-crystal-clear view.

As the patrol agent in charge of the Sanderson Border Patrol Station, I worked with Sheriff Ronny Dodson of Brewster County, former Terrell County Sheriff Clint McDonald to develop a network of BuckEye game cameras that shared real-time images to our respective offices. This was a collaborative effort to enhance border security and was the first effort of its kind along the U.S./Mexico border.

Also, during my command of the Border Patrol Station in Sanderson, Texas, we received and deployed our first 8 Autonomous Surveillance Towers. This is an incredible asset, yet we quickly learned they detected more activity and we did not have the manpower to pursue everything the towers revealed. With that being said, you can have as much technology on the border, but without the right balance of manpower, the technology is useless.

The State of Texas is also utilizing various technology platforms along the U.S./Mexico border. In 2008, I was assigned as U.S. Border Patrol's representative to the State of Texas, during this time, Texas Department of Public Safety first deployed their Drawbridge game cameras along the along the U.S./Mexico border. This program now has over 7,000 game cameras along the border. The State of Texas has also constructed over 40 miles of border wall in Texas and has mounted camaras systems on the wall as well.

As Sheriff, through Operation Lone Star, my office has been able to receive night vision and thermal imaging devices and we are waiting on approval of 3 Mobile Video Surveillance platforms.

I think defining success for border security initiatives at the county level involves a collaborative approach and setting realistic, localized objectives. Success at the county level is measured by our ability to effectively utilize limited resources to enhance security and reduce illegal activity. This means fostering strong partnerships with Federal and State agencies, maximizing the impact of every dollar spent, and ensuring our personnel are well-trained and equipped.

One key indicator of success has been our effective use of grants and State programs. For example, through Operation Lone Star and Operation Stone Garden, we've been able to hire additional deputies, acquire new vehicles, and obtain vital technology like thermal cameras and night vision equipment. These resources have significantly bolstered our capability to patrol and secure the border.

Our success is also evident in the reduced level of illegal activity in Terrell County. By taking control of the highways and leveraging surveillance technology, we've deterred illegal crossings and forced smugglers to reroute further north, avoiding our jurisdiction. This shift is confirmed through intelligence reports and feedback from sources on the ground.

At the Federal level, success is often measured by broader metrics, such as overall apprehension numbers and the implementation of large-scale infrastructure projects. The Federal Government operates with a much larger budget and a focus on Nation-wide border security strategies. In contrast, at the county level, we work with more constrained budgets and focus on immediate, localized impacts.

Ultimately, success for us is defined by our ability to protect our community efficiently and effectively, using available resources and strong partnerships to fill gaps where Federal and State support is limited. This local perspective ensures that we address specific threats and challenges unique to our region, contributing to the overall border security efforts in a meaningful way.

The chaos along our Southwest Border is solvable and preventable. Solutions exist, they need only ask those of us on the ground dealing with this every day. The border is open, overrun, and the criminal organizations are taking full advantage of our political gridlock.

To secure our borders we must go back to securing the areas in between our Ports of Entry. To do this, added resources such as manpower, technology, and infrastructure are required to detect, track, and apprehend those who mean us harm. Additionally, we must always be prepared for a mass migration crisis. We must bolster our current infrastructure to include the addition of more detention centers that are used for short- and long-term detention of illegal aliens, that include immigration judges at each location to expedite immigration hearings.

Ports of Entry along the Southwest Border should be designated for specific needs such as political relief, natural disasters, and work-related industries.

Border Security and Immigration Reform are separate and individual issues. They should be kept and managed separately as border security does not just focus on illegal immigration. Border security is paramount to national security.

To ensure the security of our Nation, those of us that have sworn an oath to protect and defend the Constitution of the United States must come together to develop, implement, and execute viable solutions. This is why I am in speaking to you today. The advancement of technology has been key to securing America's border. Technology coupled with the ingenuity of Border Patrol agents will continue to grow America's advancement of border security. Partnerships and leveraging technologies at the Federal, State, and local level is also necessary to keep American and American's [sic] protected.

Mr. HIGGINS. Thank you, Sheriff Cleveland.

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

STATEMENT OF CARL LANDRUM, VICE PRESIDENT, CIVILIAN PROGRAMS AND STRATEGY, DEDRONE

Mr. LANDRUM. Thank you, Chairmen Higgins and Bishop, Ranking Members Correa and Ivey, and distinguished Members of the subcommittee.

Thank you for the opportunity to testify on behalf of Dedrone. I hope my testimony will help the subcommittee better understand the rapidly-evolving threats in the air space above our international borders and that sophisticated technological solutions exist to counter these threats and to keep Americans safe.

My name is Carl Landrum, vice president of Civilian Programs and Strategy at Dedrone, the U.S.-based global provider of state-of-the-art air space security solutions with the mission to protect people and property from malicious drones while enabling the good drones to fly.

Prior to Dedrone, I served nearly 3 decades in DHS, starting as a Border Patrol agent in 1996. During my career, I witnessed the use of drones by cartels, transnational criminal organizations, also known as TCOs, for drug trafficking, reconnaissance, and surveillance while noting a lack of technologically-based drone detection capabilities within the Border Patrol.

Until my retirement in 2023 as a chief patrol agent and including my present work in industry supporting U.S. Government customers, I have experienced first-hand the tremendous evolution of drone usage by TCOs to further their illicit and deadly activities. Over the same time, the U.S. Government's counter-drone technology at the border has struggled to keep pace.

To close this capability gap, Congress must ensure that CBP has sufficient resources to leverage commercially-available technologies that can counter TCO drone operations. This investment must be significant, and it must happen now as nefarious actors around the world are rapidly advancing their drone operations and exporting capabilities to our borders.

In the early days of the Ukraine conflict, Dedrone's counter uncrewed aerial system, also known as C–UAS, was deployed a crucial role in detecting drone activities. However, as the conflict progressed, the techniques, tactics, and procedures, or TTPs, used by both Russia and Ukraine have evolved at the speed of war, rendering traditional radiofrequency, or RF, detection methods such as decoding infective.

Russia's ability to manipulate and conceal the RF signatures from its drones through technologies like spoofing, cloning, and even autonomous flight has made the sole reliance on decoding unreliable.

Rooted in a long-standing tie between Russia and certain countries in South America, we have begun to see some of these TTPs arriving in the Western Hemisphere and making their way to our own borders. Cartels in Mexico have billions of dollars to invest heavily in sophisticated drone tactics, learn from conflicts abroad. These tactics include drone-mounted improvised explosive devices, and DMIEDs are already being used on the Mexican side of the border today.

This past January, Dedrone entered into a contract with CBP at no cost to the Government to perform a long-term demonstration of C–UAS capabilities along a 5-mile stretch of the U.S. border in Laredo, Texas. To date, Dedrone has invested over $3.3 million to establish a multi-layer C–UAS detect, track, and identify, DTI, capabilities, including radiofrequency radar and camera sensors, as well as software powered by AI, including machine learning and computer vision.

The Laredo demo can detect nearly 600 different drone models, including both hacked and home-made drones. In the first 80 days of the Laredo demo, we identified approximately 2,400 flights in the air space. DJI drones, detections represented 71 percent of those alerts.

Additionally, 16 other drone manufacturers were detected in the air space. This multi-layer solution of RF plus radar, plus camera, combined with AI-driven sensor fusion has provided CBP complete air domain awareness along these 5 miles of border.

Without Dedrone's larger investment, 29 percent of drone flights in this air space would have gone undetected.

Thank you again for the opportunity to testify, and I look forward to answering any questions you may have.

[The prepared statement of Mr. Landrum follows:]

PREPARED STATEMENT OF CARL LANDRUM

JULY 9, 2024

INTRODUCTION

Chairmen Higgins and Bishop, Ranking Members Correa and Ivey, and distinguished Members of the subcommittees, thank you for the opportunity to testify before you today on behalf of Dedrone. I hope that my testimony will help the subcommittees better understand the emerging threats in the air space along our international borders and that sophisticated technological solutions exist to counter these threats.

My name is Carl Landrum and I am the vice president of civilian programs & strategy at Dedrone. Dedrone is a U.S.-based global provider of state-of-the-art air space security solutions with the mission to protect people and property from malicious drones, while leveraging technology to allow good drones to fly. Prior to joining Dedrone last year, I had the honor and privilege to serve as a law enforcement professional and senior leader in the Department of Homeland Security (DHS) for nearly 3 decades. I began my career in 1996 as a Border Patrol agent in San Diego, CA. After the tragic events on September 11, 2001, I transferred to become a Federal Air Marshal from 2003 to 2005, and then transitioned back to the Border Patrol. Over the course of my 27 years with DHS, I had the opportunity to work in various roles in multiple sectors along our Nation's international borders, including as the deputy chief patrol agent of the Yuma Sector in Arizona and as the chief patrol agent of the Laredo Sector in Texas.

Beginning in 2015, while I was serving as the deputy chief in Yuma, I personally witnessed the genesis of the use of drones by trans-national criminal organizations (TCOs)—also known as cartels—operating on both sides of our international border with Mexico. In those early years, the cartels conducted simple trafficking operations using drones. For example, we observed and recovered drones flying short distances from Mexico into the United States carrying small amounts of methamphetamine and black tar heroin. Oftentimes these drones would crash land in backyards demonstrating the initial lack of knowledge, skills, and capabilities. At that time, the Border Patrol had no technology-based drone detection capability whatsoever.

From 2015 until my retirement in 2023, and to include my present work in industry supporting U.S. Government customers, I have experienced first-hand the tremendous evolution of the usage of drones by TCOs to further their illicit and deadly activities. While over the same period of time, the U.S. Government's counter-drone technology and capability has lagged far behind. To close this growing capability gap, Congress must ensure that U.S. Customs and Border Protection (CBP) has sufficient resources to leverage commercially-available technology and capabilities that can counter TCO drone operations. This investment must be significant, and it must happen now, as nefarious actors around the world are rapidly developing and advancing their drone operations and exporting them to our borders.

FROM EASTERN HEMISPHERE TO WESTERN HEMISPHERE

Since the early days of the on-going conflict in Ukraine, Dedrone's counter unmanned-aerial systems (C–UAS) have been deployed on the ground along the front line in what has grown into a full-scale drone war between Russia and Ukraine. The tactics, techniques, and procedures (TTPs) used by both countries have rapidly evolved at the "speed of war" over the past 2 years and observing these TTPs first-hand continues to provide us with incredibly unique and informative insights and lessons into present and future drone warfare. At the beginning of the war, "advanced" radio frequency (RF) detection, also known as RF decoding, similar to what is still used on the U.S. borders today, was the primary capability used to detect Russian drone operations and attacks. Today that methodology of drone detection is wholly insufficient and no longer the case in Ukraine. Russia's ability to manipulate and conceal the RF signatures emanating from its drones, through TTPs such as spoofing or cloning, or even fly autonomous drones, means that relying on RF decoding alone for drone detection and location is quickly becoming unreliable and obsolete.

RF decoding reads the RF signal communications between the drone and its remote control to extract data such as GPS coordinates (if available), altitude, and speed. However, there are many limitations to relying solely on decoding as part of a C–UAS apparatus.

- *Encryption.*—Many drones encrypt their RF signals to avoid being located. These encryption keys can be easily updated and changed to ensure that decoding remains not only expensive but also unreliable. The moment it is known that an RF signal is understandable, the manufacturer or user can simply leverage a new encryption mechanism.
- *No Location Offered.*—Not all drones come equipped with GPS microchips installed. Therefore, if there is no GPS board then there is no coordinate data to extract even if decoding is possible. This non-existent GPS board issue is particularly true when it comes to home-made drones.
- *Spoofing.*—Unencrypted drone data can be susceptible to tampering. The concern lies in the potential manipulation of data transmitted by drones, a tactic known as spoofing. Spoofers can alter drone signals, making them appear to originate from a different location or masquerade as another drone altogether.

Additionally, spoofers can easily generate a drone signal where there is no drone at all. This presents a substantial hurdle in drone detection efforts, especially when solely relying on RF decoding techniques.

- *Autonomous*.—Some drones can be pre-programmed to fly a specific route ahead of launch. With these drones there is no RF signal to direct the drone during flight and thus no RF signal to detect/decode.

Presently, Dedrone observes all these TTPs being implemented on both sides of the conflict in Ukraine to hide the true location of drones. As these TTPs become perfected on the battlefield, it was only a matter of time before these TTPs permeated from the front line in Ukraine into the Western Hemisphere and along our Southwest Border. The TCOs operating along and south of our border with Mexico generate tens of billions of dollars each year in revenue from their illicit activities. With this endless supply of funds at their disposal, the cartels invest significant resources into the latest and most sophisticated drone-related TTPs that will further their illicit activities and generate more profit.

Rooted in long-standing ties between Russia and certain countries in South America, we are beginning to see some of these same TTPs arriving in the Western Hemisphere and making their way to our own U.S. borders. According to open-source media reporting, in October of last year, 8 Colombians were arrested in Jalisco, Mexico for constructing improvised explosive devices to be used as payloads on drones for a local criminal gang involved in narcotics trafficking.[1]

I have personally observed the steady maturation of the TCOs' drone operations and use of technology on both sides of the U.S.-Mexico border to thwart CBP's very limited drone detection capabilities.[2] Even out-going Mexican President López-Obrador over the past year has openly called for greater international assistance to help Mexico with its drone problem.[3]

U.S. BORDERS LACK AIR SPACE SECURITY

At present along our international borders, the Border Patrol maintains only basic C–UAS capability, using only decoding RF methodology to detect, track, and identify (DTI), from only a single manufacturer, DJI. For context, Dedrone maintains a library of over 150 unique drone manufacturers, from our deployments around the world. Additionally, even with just this basic DTI capability deployed along our international borders, there have been approximately 37,423 flights detected near the border (within 400 meters) in fiscal year 2024 year-to-date (YTD), of which >2,492 of those drones flew illegally across the border.

Along our Southwest Border specifically, the use of drones by the TCOs is growing at a rapid rate as they innovate to further their illicit activities. Drones are currently being used by TCOs and other illicit bad actors to:

- Conduct surveillance of U.S. Government personnel and facilities along the international border;
- Conduct counter-surveillance on rival TCO and government of Mexico (GoM) military positions;
- Provide overwatch and guide groups of migrants attempting to avoid apprehension;
- Provide overwatch and guide individuals and groups smuggling narcotics into the United States;
- Physically drop narcotics via drone delivery across the border;
- Physically drop bundles of currency as payments to individuals on the U.S. side of the border.

At the same time TCOs are using drones more frequently, they are also continuously altering their technologies and methods, and flying many different types of drones to defeat USBP's very limited DTI capability—specific to only non-tampered DJI drones. At present, Border Patrol agents have virtually zero capability to detect non-DJI, modified DJI, or encrypted DJI drones.

LAREDO DEMO

In January of this year, Dedrone entered into an official contract with CBP—at no cost to the Government—to perform a demonstration project of C–UAS capabili-

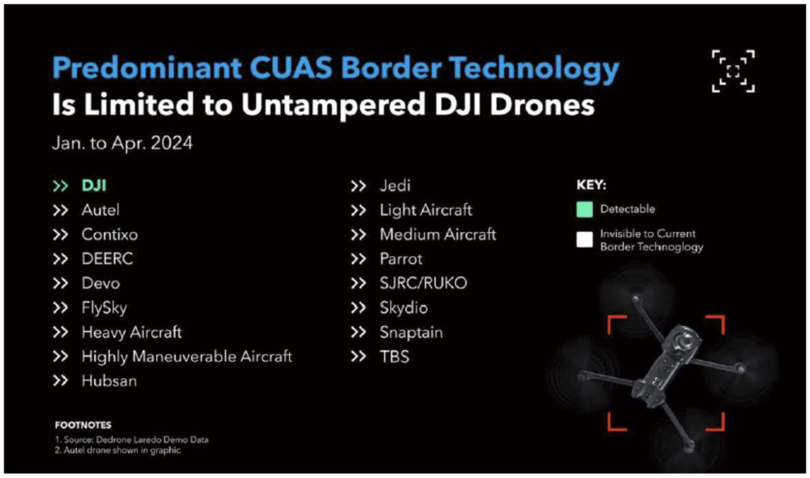
[1] Narcosis, *8 Arrested in Mexico For Manufacturing Drone Explosives,* ATLAS NEWS (Oct. 9, 2023).

[2] *CJNG attack against indigenous community of Michoacán denounced,* EJECENTRAL (Jul. 4, 2024). Mark Stevenson, *Mexican cartels now use IEDs as well as bomb-dropping drones,* ASSOCIATED PRESS (Feb. 4, 2022). Gabriel Mondragon Toledo, *NarcoDrones Have Become a Growing Scare Tactic in Mexico's Drug Wars,* INKSTICK (Nov. 7, 2023).

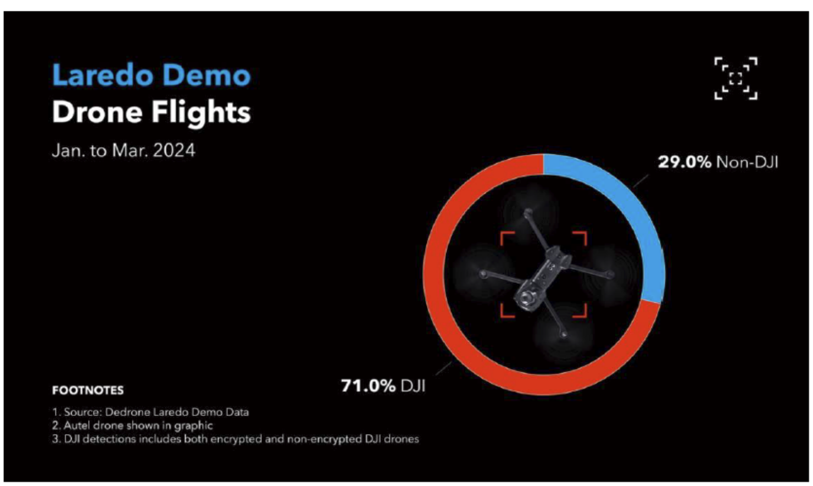
[3] Julian Resendiz, *AMLO seeks enhanced penalties to curtail drone attacks,* NEWSNATION (Aug. 10, 2023).

ties along a 5-mile stretch of the U.S.-Mexico border in Laredo, TX. To date, Dedrone has invested over $3.3 million to establish full spectrum C–UAS DTI capabilities including RF, radar, and camera sensor hardware, as well as software powered by artificial intelligence (AI), including machine learning and computer vision. This Laredo Demo can detect nearly 600 different drone models including altered drones and even homemade drones.

In addition to non-tampered DJI drones, the Laredo Demo project also detected the following drone types:



In the first 80 days of the Laredo Demo, Dedrone detected 682 unique serial numbers operating along this 5-mile section of the border. It is important to note that this accounted for only 71 percent of the total drone detections made during this period. There were an additional 16 drone manufacturer types that would NOT have been detected but for the Laredo Demo project. These detections comprise 29 percent of the total made during this period and would not have been detected prior to the Laredo Demo. The full spectrum of sensing capability—RF, radar, and camera—combined with the AI-driven sensor fusion, temporarily deployed by Dedrone, allow CBP to have complete air domain awareness along these 5 miles of border. Without it, CBP is limited to their basic DTI capability—specific to only non-tampered DJI drones—and would be blind to 29 percent of all drone flights.



RECOMMENDATIONS FOR CONGRESS

C–UAS Authorization Legislation

- We strongly urge Congress to enact comprehensive C–UAS authorization legislation this year to ensure that CBP's C–UAS authorities to protect people and property continue well into the future.
- We applaud Chairman Green and Ranking Member Thompson for their leadership and tireless work on H.R. 8610, the Counter-UAS Authority Security, Safety, and Reauthorization Act, and we strongly support the framework and principles of the bill.
- Any authorization must include a multi-year renewal of Federal authorities.
  - As is envisioned in H.R. 8610, Congress should enact a multi-year extension and enhancement of C–UAS authorities under 6 USC 124n for Federal Government agencies like CBP.
  - Providing agencies with adequate certainty over multiple years will allow for better planning and budgeting for C–UAS programs and activities.
- H.R. 8610 also contains provisions that clarify the rules for how and when law enforcement can utilize RF decoding to DTI unauthorized drones. While RF decoding has its limitations, it remains a useful tool, and it is vitally important to clarify the policies law enforcement must adhere to.

DHS Appropriations

- Increase funding for the procurement of C–UAS capabilities by CBP.
  - As the subcommittees know, the House recently passed a DHS Appropriations bill for fiscal year 2025 that included a generous increase in funding to enable CBP to procure additional C–UAS capabilities. Thank you for this very timely and important investment in our border security.
  - Based on my 3 decades of experience executing and leading border security operations, including the past 9 focused on C–UAS threats and capabilities, it is my view that CBP requires a $1 billion program of record to counter current and emerging threats, and achieve appropriate air space security along our international borders.
  - Based on this metric, I believe that Congress should appropriate $250 million as an initial down payment for the procurement of CBP C–UAS capabilities.
- Congress should direct and encourage CBP to fund C–UAS programs and activities that move beyond single manufacturer RF decoding including:
  - Expand RF sensing to DTI all RF based drones including spoofed or encrypted drones as well as homemade drones. As previously described, there are many limitations to relying solely on decoding as part of a C–UAS apparatus.
    - Full RF sensing includes localization through different types of triangulation (ie: angle of arrival and time difference of arrival) to offer a more fail-safe way to detect and locate drones.
      - *Angle of arrival (AOA).*—Using this method, one sensor can be used to determine the direction of the drone and multiple sensors can be leveraged to calculate the exact position of the drone based on triangulation from multiple direction sensing sensors.
      - *Time difference of arrival (TDOA).*—This method measures the difference in time of arrival between several sensors. TDOA depends on the distance between the drone and sensors.
  - Further enhance DTI capabilities to detect autonomous drones (no RF signal) and drones at greater distances by bringing long-range radar and long-range camera (for visual confirmation and payload detection) into a single fused instance from these multiple sensor types.
  - Enhance non-kinetic mitigation capabilities to allow CBP personnel to safely address unauthorized drone activity.
    - Develop and deploy advanced jammer-based mitigation that is effective against single drones as well as drone swarms (defined as more than one drone) and sustainable as the threat seen around the world evolves in the United States.

Thank you again for the opportunity to testify and I look forward to answering any questions you may have.

Mr. HIGGINS. Thank you, Mr. Landrum.

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

STATEMENT OF DAVID J. BERTEAU, PRESIDENT AND CEO, PROFESSIONAL SERVICES COUNCIL

Mr. BERTEAU. Thank you, Mr. Chairman. Thank you for the opportunity to be here, Chairman Higgins, Chairman Bishop, Ranking Member Correa and Ranking Member Ivey, and the rest of the Members of the committee. It's a great privilege for me to be here today.

I represent the Professional Services Council, as you noted in our opening statement, Chairman Higgins. That's over 400 member companies. It's large, medium, small companies, and we cover only Federal Government contracting. That's our focus, is how does the Federal Government get more out of the private sector? To do that, I want to emphasize the partnership.

I'd like to deviate a little bit from my statement and respond to some of the comments that each of you raised in your opening remarks and talk about how we come into play there.

Chairman Higgins, you raised the real issue right at the beginning, right? The threat is evolving faster than our ability to acquire and use the technology. It's not that technology isn't developing fast enough. It's that the Government processes to put the requirements in place, this is what we need, to get the funds in place, get Congress to authorize and appropriate those funds, and then actually issue the contracts and administer those—that's a long period of time. So you put your finger on it right there. We got to move faster because the threat is evolving faster to take use of that technology.

Mr. Correa commented about tech is not enough. You got to have the people. I think that when we look at—I believe Mr. Ivey, you mentioned AI as a supplement to that. It's not to replace people. It's to actually use the time that people have to be more effective. That's one of the real challenges we have because we can overwhelm ourselves in that regard.

Mr. Bishop, you focused on what really matters a lot to me, which is streamlining the acquisition process so you can actually get to results faster—right?—and to increase that partnership. We've got a number of recommendations that we come into play there.

So let me—let me just say, from PSC's, our 3 main goals—and they're not just goals for technology at the Government. They're goals for the whole Federal Government—our goal is to help make the Government a smarter customer. By that we mean better able to know what they can get, what's out there.

You know, they come looking to you—I mean, the first thing that the Government will say is, well, I don't have a requirement for that. That's because they didn't know you could do it. So make them a better—a smarter customer. Make them a better buyer, better able to go get it faster. But, more importantly, streamline the process so you can get technology at the pace it's developing.

Then, finally, all of you mentioned the connection to the work force. If you don't have the people, it doesn't matter what the technology is going to do.

So we have 4 suggestions that we make for this Congress and for DHS to do that, and I'll be glad to go into those in more detail in my—in the questions here.

No. 1 is that we believe DHS should focus its contract requirements more on results and outcomes—what do I want to get done with this contract—rather than on inputs. I'm going to buy so much time, so many labor hours, so many labor categories, et cetera.

No. 2 is Congress can support long-term commitments better by passing appropriations on time. When you don't get your appropriations until March 23, and then it takes OMB a month to apportion it down to headquarters, and it takes headquarters another month to apportion it down to CBP, you've got 3 months left in the fiscal year to spend the money. You can get the technology faster, DHS can deliver the results faster if we appropriate the funds on time.

The third is that contracts take too long, and we think Congress can help DHS speed up the time it takes to award contracts. I'll be glad to elaborate on that a little more during the questions.

Then, finally, in the end, you know, innovation and technology doesn't do any good if people can't use it. So you need to train, you need to take into account how people are going to use it as part of that process. You know, innovation that we don't use is not a solution. It's just an additional problem to come into play.

So we think a lot more emphasis needs to be on training for use and a focus on use when we acquire that technology.

With that, gentlemen, I'll close my remarks and tell you I'm grateful for your time and consideration of these matters, and I look forward to your questions.

[The prepared statement of Mr. Berteau follows:]

PREPARED STATEMENT OF DAVID J. BERTEAU

JULY 9, 2024

INTRODUCTION

Chairman Higgins, Chairman Bishop, Ranking Member Correa, Ranking Member Ivey, and Members of the committee, thank you for the invitation to testify on the role of technology and innovation in our Nation's border security strategy.

I appear before you today on behalf of the Professional Services Council (PSC). We are a trade association of companies that do business with the Federal Government, with more than 400 member companies and hundreds of thousands of employees across the Nation. PSC represents the full scope of the Government contracting sector, with companies of all sizes (small, mid-sized, and large). Our member companies work in partnership with every Cabinet department and agency, supporting every mission and function of the Federal Government.

I am here not just as the head of PSC but also as a person with more than 40 years of experience on these issues from all sides, including two stints inside the Pentagon as well as with industry, at a think tank, in academia, and now in my ninth year at PSC. I have run contracts that undertake to bring technology to border security and to the broader challenges of national security and addressing the Government's needs. I have worked with State and local governments in partnership with Washington. I have seen the challenges that both sides face, and I have worked to provide what is needed to improve acquisition outcomes. In particular, I have long wrestled with how Federal agencies can find, acquire, and use new technology and innovative processes and systems.

PSC's member companies provide the full range of technology and professional services to all Federal agencies that pertain to our air, land, and sea border-related issues. Within the Department of Homeland Security, their customers include Customs and Border Protection (CBP), the U.S. Coast Guard (USCG), the Transportation Security Administration (TSA), and Immigration and Customs Enforcement (ICE). They also support agencies beyond DHS, including for example the Office of Refugee Resettlement (ORR) in the Department of Health and Human Services and the Justice Department's Executive Office for Immigration Review (EOIR) as well as many other programs and agencies.

PSC member companies help the Government acquire and use multiple technologies, including detection systems, communication systems and networks, artificial intelligence and data analytics, UAS (unmanned aerial systems) and counter-UAS, case management, information technology systems and infrastructure, and many other vital and emerging technologies needed for border security.

The diversity of contracts and customers, the range of solutions provided, and the size and reach of PSC member companies give us broad and deep perspectives on the challenges involved with identifying, procuring, and implementing technology and innovation to secure our borders and the important partnership role that our members and all of industry has in supporting border security in all its dimensions.

In fiscal year 2023 (FY23), DHS obligated more than $25 billion on contracts, including:

- $7 billion for CBP,
- $2 billion for TSA,
- more than $3 billion for ICE, and
- $1.4 billion for USCIS.

Both new and legacy technology needs make up a significant part of those contract dollars, playing essential and critical roles in protecting and securing the border. These contracts represent the partnership of Government and industry, working together on the same goal—to develop and acquire the capabilities needed for mission success through systems and processes that are timely, cost-effective, and accountable. That partnership operates within Federal acquisition rules and regulations that encourage competition, innovation, and investment in the homeland security marketplace.

PSC GOALS FOR THE GOVERNMENT-CONTRACTOR PARTNERSHIP SUPPORTING TECHNOLOGY AND INNOVATION

At PSC, we support this Government-contractor partnership by focusing on three goals:

- making the Government a smarter customer and a better buyer (i.e., knowing what to buy and how to buy it),
- improving contracting procedures to support technology modernization and innovation, and
- supporting policies and practices that build and sustain the workforces needed to meet Government missions, both for our member companies and for their Government customers.

First is to help the Government become a smarter customer and a better buyer, leading to improved acquisition outcomes. Being a smarter customer means knowing what is available from every source, including the private sector, the national economy, and around the world. Being a better buyer means that, once the Government identifies a product or service they can use, being better able to get the funds and procure that product or service. Both goals need to focus on getting better results for the Government, consistent with its needs.

Second is to support technology modernization and innovation through contracts. The Government is not alone in being able to find and get innovation and new technology. Contractors can and do play vital roles in extending the Government's reach, capability, and capacity. I will have more to say on these vital roles later in this statement.

Third is to support workforces needed to meet Government missions, both for our member companies and for their Government customers. Better and more relevant training is an important part of workforce development and retention, and it is one of the areas that Government contractors can strongly support. These goals are particularly important in all the areas affected by border security, where shortages of trained, experienced personnel is a long-standing issue.

In summary, the overall goal of PSC and our member companies is to help the Government operate better, improve outcomes and results, and achieve its missions. These goals are particularly important in all aspects of achieving border security.

KEYS TO A COMPREHENSIVE AND SUCCESSFUL STRATEGY

Next, I want to touch on the elements of a successful border security strategy. My Pentagon experience taught me that a successful strategy needs to address ends, ways, and means. Most importantly, a strategy is only as good as its implementation. A key element of successful implementation is for the strategy to include finding and using technology and innovation to support its goals.

"Ends" are the objectives, both as a final state and as the strategy is being followed. What are the goals?

"Ways" are the actions and reactions taken to pursue the strategy's objectives. What do you do, and particularly what do you do differently?

"Means" are the resources needed: The people, the equipment, the funds, the support, and the innovation and technology.

In essence, a strategy is a detailed plan, with goals, planned actions, and resources. Designing, issuing, and implementing any strategy, including a border security strategy, is a joint responsibility of the Congress and the Executive branch, but it also depends on that Government-industry partnership. Let me highlight some of the roles contractors play in setting and implementing strategy.

Our member companies do not develop or promulgate the Government's strategies. They do not set the goals and objectives. Setting goals and defining the objectives (the "ends") of any strategy is the Government's job, what the Office of Management and Budget calls "inherently Governmental functions."

It is also the Government's job to lay out the actions and reactions taken to pursue the strategy's objectives, the "ways" of the strategy.

The "means" are also set partially by the Government. Executive branch agencies set up the offices and programs and, through the Congress, secure the funding, part of the "ways" of the strategy.

Where contractors come in is providing some of the rest of the "means," including the necessary people, equipment, facilities, and support. Throughout the implementation of a strategy, adjustments will be needed. On the border, for example, closing one access point might lead to increased use of another access point, requiring shifts in resources and activities. It is in that adjustment and adaptation where technology and innovation can play a big role, and contractors are also the broadest and deepest source of technology and innovation to help that adjustment. Let's look at that more closely.

TECHNOLOGY AND INNOVATION

At PSC, we connect the words "technology" and "innovation" to focus on technology solutions and innovation in systems and processes. Innovations can be changes in operations, improvements in integrating data, upgrading communications systems and networks, or cutting the time needed for a specific action. Often, the two (technology and innovation) go together. Incorporating a new technology can require, for example, changes in procedures, updates in training, or alternate ways to exchange data or to communicate.

Recent years have seen a call in the Government for more innovation. This includes greater access to companies in the private sector, including companies with no prior Federal Government business. That approach should be part of the Government's pursuit of innovation, but it's not enough. The Government also needs to improve its use of today's contractors as a path to greater use of technology and innovation.

Why is that? It is because doing business with the Federal Government is not the same as doing business in the commercial market. Contractors are funded with taxpayer dollars, and the American public expects tighter, more rigorous Government rules and regulations for Federal contractors than for other private-sector companies. Congress regularly responds to instances of contractor misconduct by updating or expanding laws that flow through those regulations.

These rules mean that companies that do business with the Federal Government must comply with myriad requirements and produce reports that depend on accounting systems, billing processes, employee time keeping, and detailed information far beyond those needed for commercial business. The Government often requires contractors to provide access to their proprietary intellectual property, their software code, or their trade secrets.

All of these compliance requirements are designed to support Government goals, but they often contribute little to actually delivering results under a contract. In general, purely commercial companies do not need or have the systems and processes in place to certify compliance with Government contracting requirements. Since failure to comply often can incur civil and criminal penalties and even result in a company being debarred from future Government contracts, these rules add costs and time and are therefore a disincentive for commercial companies to compete.

Since existing Government contractors already have those compliance systems in place, they are in a better position to help their Government customers identify useful new technology and innovation and to work with the Government to modify existing contracts to incorporate that new technology into delivering better results. Using existing contractors to identify and incorporate technology and innovation can reduce the risk for the Government, help target new technology and innovation to those aspects of the mission where they will produce the greatest benefit, and provide improvements without the time-consuming effort to award new contracts.

The bottom line, then, is that both new and existing contractors can help the Government incorporate technology and innovation to meet mission needs, including border security.

A MULTI-LAYERED BORDER SECURITY STRATEGY

A multi-layered border security strategy needs to include the necessary ends, ways, and means of any good strategy. But what would a multi-layered border security strategy need to cover?

It's critical to address the immediate zone of border crossings (detection, identification, interception, etc., both at or away from authorized ports of entry) of both the Southern and Northern Borders as well as coastlines and airports, but a multi-layered strategy is more useful if it covers additional topics, including but not limited to, for example:

- U.S. needs for better intelligence before individuals arrive at any border
- entry points that are not at the land boundaries of the Nation (air, sea)
- drugs or other unwanted materiel arriving in small packages or in containers (or via drones)
- tracking people, processing cases, and managing and reducing case backlogs
- detention, housing, and medical care, etc., of individuals.

This broader, multi-layered approach would involve more than CBP to include not only the relevant agencies and components of the Federal Government but also State and local governments and other nations. In all of these interactions, a multi-layered strategy would be better to the extent it incorporates new technology and innovation in products, systems, and processes, leading to better success across the broad definition of "border security."

Most importantly, for border security, a multi-layered strategy needs to be more than simply "ends, ways, and means." The actions (the "ways") and the resources (the "means") need to be integrated, tied together in a common operating picture and interoperable, accessible, and useable by all players. Doing that demands better use of new technology and innovation across the board.

WHY IS IT HARD FOR THE U.S. GOVERNMENT TO USE TECHNOLOGY AND INNOVATION?

It is hard to get the Government to see the value of new technology, new systems, and new processes, to allocate scarce funds to buy and use them, and to change how it operates so that it can realize the advantages of that innovation. Why is this so hard? Here is what I've learned.

(1) It is hard for the Government to identify or become aware of applicable and relevant new technology, systems, and processes;

(2) It takes time (years) to plan, program, budget, and get Congress to provide the necessary funding to procure and use technology and innovation;

(3) It takes more time to solicit, evaluate, and award the contracts or buy the technology; and

(4) It takes still more time to get the Government personnel at all levels to deploy and use the new systems and processes and technology.

Using existing contractors, as noted above, can cut some time from these steps, but it still takes too long.

What, then, do we suggest will address all the issues outlined above?

PSC SUGGESTIONS TO IMPROVE ACCESS TO AND USE OF TECHNOLOGY AND INNOVATION

PSC draws on the experiences of its member companies as they undertake to identify innovations and new technology, offer them to the Government, and incorporate them into on-going operations. Based on that, we offer the following suggestions as ways to improve access to and use of technology and innovation.

(1) Earlier and More Comprehensive Identification of Innovations and Technology for Border Security

DHS components can improve their ability to find useful technology and systems and process improvements through actions such as:

- Focus their requirements, both for contracts and for operations, on results and outcomes, not just on inputs, and promulgate those requirements publicly so that companies can work to develop technology to meet them. Update the requirements often to incorporate available innovation.
- Develop and make publicly available a long-term (e.g., 5-year) investment plan and update that plan regularly.

- Expand communications with industry and encourage both existing and potentially new contractors to offer solutions. Give feedback to those offerings.

(2) Support Long-Term Resource Commitments and Increase Flexibility for Existing Resources

DHS can improve its use of existing funding and justify the need for additional funding. These suggested steps and improvements may help.

- Border security will be substantially improved if Congress appropriates funds on time, by the beginning of the fiscal year, avoiding continuing resolutions or the disruptive threats of a Government shutdown. On-time appropriations will enable DHS components to access technology and innovation faster and get results sooner.
- DHS can use existing reprogramming authority earlier and more often in the fiscal year to address emerging needs and opportunities. (Note that this needs support from both the White House and Congress.)
- Use multi-year funding and contracts to support key investments in new technology.

(3) Speed Contract Awards

An age-old problem with the Government is that, when contracts take too long to put in place, by the time new technology is procured, it will no longer be new. Recent data show clearly that, across the Government, the time between a contract solicitation and the award of that contract has been getting longer. In addition, delays appear to be increasing in the period of time before a solicitation is issued. Both of these problems need attention by DHS and Congress.

Congress can help by conducting oversight hearings that illuminate both the increased time consumed by contracting and the causes and possible fixes to reduce that time. Congress can also help by requiring annual reports from DHS on procurement and administrative lead times for all types and sizes of contracts.

(4) Training To Use New Technology

We all know how hard it is to adapt to an upgrade or an innovation in something that we are used to, whether it's using a new cell phone, the latest version of the operating system of a laptop, or the features and controls of a new car. This same dynamic exists when any agency or component incorporates new technology and innovation into existing operations.

To offset this natural occurrence, DHS components could plan for and fund the time, the resources, and the capacity and capability to train the workforce to take advantage of new technology. Contractors can help develop and provide that training more rapidly and broadly.

CONCLUSION

In closing, on behalf of PSC and our members, I thank you for your time and consideration of these matters. PSC member companies are proud to work with CBP, with DHS, and with other Federal departments and agencies to provide technology and increase innovation for border security. We are committed to the missions.

As always, PSC is available at your convenience to address any questions or concerns the committee has, now and in the future. I will try today and for the record to answer any questions you may have, and I look forward to continuing to work with the committee and these subcommittees on these issues. Thank you.

Mr. HIGGINS. Thank you, Mr. Berteau.

Members will be recognized by order of seniority for 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. Landrum, would you clarify for the committee and for the Americans that are watching regarding drone technology? In my limited time, it's just what I'm going to focus my questions on for you gentlemen.

Regarding drone tech and anti-drone tech, will you explain the difference between defensive and offensive capabilities for anti-drone technology for America?

Mr. LANDRUM. Yes, sir. When it comes to C–UAS capabilities—which is what you're referring to—there are 2 big portions of that.

One of them is the ability to detect, track, and identify a drone that is flying in an air space that is being covered by that particular technology.

Mr. HIGGINS. Is what I'm referring to—not to interrupt, but that we would call defensive drone technology. Would you explain offensive drone technology?

Mr. LANDRUM. Yes, sir. That side of it is referred to as mitigation. Mitigation can take forms of radiofrequency, so via jamming, radiofrequency jamming. It also could be kinetic; just depends on the situation. Inside the United States, kinetic is not used.

Mr. HIGGINS. So for radiofrequency interruption for a drone that's been observed by a law enforcement professional on the front line as a suspicious drone, a criminal drone, the defensive technology of our anti-drone capabilities is that we can track those drones, and we can show the history of that flight, we can identify that drone. But the full capability of anti-drone technology—I bring this us up for my colleagues across the aisle primarily, because what the administration has been telling us, what the Secretary of Homeland Security has been telling us, we're using that anti-drone technology. But he's only telling you the half-truth.

It's used in the defensive capabilities of our anti-drone technologies, not the offensive capabilities or the mitigation capabilities. So when you talk about radiofrequency interruption, you're talking about landing that drone, correct?

Mr. LANDRUM. What we are talking about with jamming—the radiofrequency jamming, which can be band jamming, spectrum jamming in some—in some cases or some technologies——

Mr. HIGGINS. What happens to that drone?

Mr. LANDRUM. What you're doing is you're breaking the connection between that drone and its pilot.

Mr. HIGGINS. Right. So what happens to the drone itself?

Mr. LANDRUM. The drone generally in every situation is different. Every single environment is different, and what's available mechanically is different.

But generally, what happens is 1 of 3 choices. Either, No. 1, that drone will be disrupted, it won't know what it's doing, so it will return to its home location automatically. No. 2, it could just come straight down to the ground. Or, No. 3, if the right circumstances existed, you could actually take control of that drone and bring it——

Mr. HIGGINS. You could take control of it. In the interest of time—I'm trying to get to here—the offensive capability of our existing anti-drone technology allows us to disconnect a criminal drone from its operator and take control of it either because we land it or we actually seize control of it.

Is this a technology that we currently have?

Mr. LANDRUM. We do have very limited amounts of that technology.

Mr. HIGGINS. OK. Sheriff, long ago when I was a young police officer, 20 years ago—I think it was 2005—one of the more interesting things that happened that week, we had an armed robbery, high-speed chase. I happened to be involved, was able to force the suspect's vehicle to crash. In the process, crashed my own car, but made the arrest.

When the supervisor showed up pretty quickly, my crashed patrol car and that crashed suspect car was not treated with a typical Louisiana uniform motor vehicle crash report. It was treated as a criminal—as a part of a law enforcement action in that response to criminal activity.

So the crash itself was documented in our investigative report, not in a typical uniform motor vehicle crash report, because it was a law enforcement action.

On the border, when law enforcement uses the offensive capabilities of our existing technology to bring down a drone, this administration wants to treat that law enforcement action as a crash to be investigated by FAA.

So this is something—we have follow-up questions we're going to deliver in writing to you gentlemen. But it's an area where I believe that this committee can come together and address the common-sense difference between a law enforcement action where a drone is taken down using existing technologies that we have versus an aircraft crash that requires investigation by FAA.

My time has expired, but my interest in this topic has not. I yield to the Ranking Member.

Mr. CORREA. Thank you. Mr. Chairman, I concur with you on this being an issue for both of us to work on, both sides of the aisle.

I want to also add to that another wrinkle in our FAA law, which is, if our locals want to take down drones, do anything with drones, right now they are prohibited from touching drones. Only a Federal authority can actually do anything of a sort to a drone.

So that means my folks back home monitoring Disneyland or an Anaheim Angels game, it's the local authorities, they have no power over bringing down a drone. So there's a lot of issues in existing law that we have to address. More in lines of, really, how do we coordinate Federal, State, and local agencies against this—you know, this danger, so to speak?

If I may, gentlemen, thank you for your comments. Mr. Landrum, I want to start with you. Yesterday we spoke, and you said you started seeing drones at the border as early as 2014?

Mr. LANDRUM. It was late 2015, 2016, 2017 is where we really started seeing this activity at the border.

Mr. CORREA. Have we reacted? Do you believe the homeland security reacted appropriately to these threats at that time?

Mr. LANDRUM. Sure. I think the reaction has—was slower than I would have wanted it to be as a Border Patrol agent on the border at the time. But there has been a reaction.

Yes, some—some equipment and some assistance has arrived to help the agents.

Mr. CORREA. You know, not only has the number of drones coming across the border increased, but you said something right now that caught my interest. You said cartels in Mexico have billions. We know they are. They have the best consumer market in the world, American drug consumers. They've got a lot of money.

But you said cartels in Mexico have billions to—and they're using explosive devices. On whom?

Mr. LANDRUM. There are multiple open-source media reports. An easy Google search can deliver dozens upon dozens of these throughout the entire country of Mexico where drones with explosives are being utilized down there. In addition to the——

Mr. CORREA. Utilized against who? Authorities or each other or all of the above?

Mr. LANDRUM. I think it's really all of the above. Definitely utilized between rival cartel positions and government of Mexico positions, but also as recently as just last Friday in my—in my longer opening statement, just last Friday, you know, a cartel attacked some local community members in a drone attack that went on for a couple of hours.

Mr. CORREA. So these are very dangerous offensive capabilities that are now being introduced to drones to be used?

Mr. LANDRUM. These are dangerous offensive capabilities that are being utilized by the cartels, and they are getting——

Mr. CORREA. As I watch what's going on on a daily basis the Ukraine war, this technology is evolving on a real-time basis. Every day somebody is coming up with a better way to hit the other side, so to speak.

I guess, Mr. Berteau, you gave us 3 ways that we could speed up the delivery of these technologies to our front line, so to speak. I'm just concerned, given what I know of the bureaucracy, both State and Federal, that we're going to need a new way to deal with this because, if drones are evolving on a daily basis, this threat to our country is multiplying as we speak.

Mr. BERTEAU. Yes, sir. I think this—both the speed and the scale of that multiplication will continue to increase over time, but I also think that American ingenuity can respond to that with the technical capabilities and the data integration necessary——

Mr. CORREA. If the bureaucracy moves out of the way.

Mr. BERTEAU. The bureaucracy has demonstrated a number of times when it can do that. One of you mentioned the other transactions authority that's available, for example, to the Department of Homeland Security to do that. I would recommend this committee take a look at it—and I'd be glad to amplify this for the record—at some of the expansions of that agreement authority that the Defense Department has been given to move from prototypes into actual production products that you can deliver.

Recently last year, in the National Defense Authorization Act, the Air Force got authority to use operations money, that is, O&M in DOD terms, to incorporate new technology into existing systems, which would speed up the process a whole lot. Because there's a lot of platforms out there that are obsolete, but you can bring new technology in as part of that.

Then the last piece of it is, actually, using the data. You mentioned noninvasive technology. I actually had a contract at Otay Mesa 26 years ago to look at sampling noninvasive technology for cars coming across the border. What happened is we quickly overwhelmed the computer's ability to actually use the data and analyze the data. We could collect data faster than we could analyze it.

Today, with artificial intelligence, the reverse is true. We're actually running out of data. We need more collection of data to be able to analyze it quickly and get it to the agents. All of those are things that would speed up the process even with the bureaucracy where it is.

Mr. CORREA. Thank you very much.

Mr. Chairman, I yield.

Mr. HIGGINS. The gentleman yields.

I recognize the Chairman of the Oversight Subcommittee for Homeland Security, Mr. Bishop, for his questioning.

Mr. BISHOP. Thank you, Mr. Chairman.

Mr. Landrum, I guess, first you—I was taken by what the Chairman was discussing about defensive and offensive capabilities and specifically offensive. First time I ever heard—and I think the number then used was, like, 3,500 flights and I've heard about 10,000 flights in a sector.

Your testimony suggested detecting—and I don't know over what period it was—but 2,400 flights in a 5-mile area, I think I heard. Is that what I heard?

Mr. LANDRUM. In a 5-mile area over an 80-day period of time.

Mr. BISHOP. So that starts to sound like even the numbers that I've heard before are small compared to what actually is happening. Am I getting the right message there?

Mr. LANDRUM. Yes, sir, you are.

Mr. BISHOP. So just a massive number of—and is this cross-border activity or just drones in the area?

Mr. LANDRUM. That number is all drone activity within 400 meters of either side of the border.

Mr. BISHOP. OK. But a lot of it is cross-border, I assume?

Mr. LANDRUM. There is cross-border. In that particular number, over that same 80-day period of time, there's approximately 146 incursions in that 5-mile area.

Mr. BISHOP. OK. So distinguish the 2 issues then for me in terms of what I ought to be concerned about as a Member of Congress.

Certainly, I—I was stunned to hear the number of cross-border flights that are allowed into their—that are happening over the American border as something I just would have assumed that whenever a drone is crossing the border and it's unauthorized, somebody would take action and stop that.

Mr. LANDRUM. There's no legal way to fly a drone over the border. That does not exist. So any drone that crosses the border in either direction has committed a violation.

Mr. BISHOP. Yet, it sounded to me that—I mean, it's not like you used—DHS uses offensive action against every unlawful crossing drone, right?

Mr. LANDRUM. That's correct, Congressman. They——

Mr. BISHOP. Why don't they? I remember at an earlier hearing, I said, well, why aren't they shot down? Ms. Titus ridiculed me for that by saying that would mean they'd be shooting drones down at Las Vegas National Airport.

I said, well, I didn't have that in mind, but out over the wilderness border area, some of the drones crossing—again, I'm not an expert. But why wouldn't there be offensive action taken against every such drone?

Mr. LANDRUM. Again, I retired a year-and-a-half ago, but I believe this statement is still true to this day. What DHS, and specifically CBP with that particular border mission, what they need is they need greater resources from this body, from Congress.

Mr. BISHOP. OK.

Mr. LANDRUM. They need those resources pushed to the border to be able to invest into these commercial technologies.

Mr. BISHOP. All right. So, Mr. Berteau, I'm going to go to you then, because you asked a—teased this issue about contracts take too long. A lot of what we're hearing and a lot of what we hear out of Ukraine, one thing that I—and even missiles and drones fired against Israel or launched against Israel, where we respond with, you know, missiles off of—fired off of ships and so forth. Their drone costs $100 and the missile costs $10 million to shoot it down, that seems like an asymmetry that we can't tolerate forever.

Comment as you will, and it will save some time for the sheriff, if you will, on the—this what you say about the contracts take too long, and are we facing a problem of asymmetry that we've got to figure out some other ingenuity to solve?

Mr. BERTEAU. First of all, Mr. Bishop, on the asymmetry, we're definitely facing that problem. I mean, obviously, you can't spend a $10 million missile to seek a $100,000 target because you're going to run out of money before they run out of targets.

Mr. BISHOP. Even in Washington.

Mr. BERTEAU. But I think technology is on our side there, our ability to actually find ways to do that. Ukraine has been an enormous test bed here.

But I also want to go back to the speed things up. So in my time in the Pentagon at the height of the campaign against ISIS and Afghanistan, we had something called the Joint Rapid Acquisition Process, right, where an urgent need could be sped up through the process with some funding that was available to both demonstrate what you could do and do it quickly. So the Government can move fast, not for everything, not for all the time.

Mr. BISHOP. Would that be the model you would look to if you were——

Mr. BERTEAU. It certainly would be a model that I would use as part of that, and I'd be happy to expand on that for the record as well.

Mr. BISHOP. Sheriff Cleveland, in the about minute I've got left, I wanted to ask you, you mentioned the word saturation at some point, saying that, essentially, you're able to use these equipment—types of equipment spot all you need, but it doesn't really make a difference in the mission, maybe, because you're taxed completely.

Speak to that, if you will, and whatever else occurs to you about what—based on what you've heard from the other witnesses.

Sheriff CLEVELAND. Yes, sir. So, as I mentioned, the Sanderson Border Patrol Station there in Terrell County has 91 miles of border they're responsible for. They're responsible for all 54 miles of Terrell County and then the southeastern portion of Brewster County.

So when you have 50 agents, approximately 50 agents patrolling 91 miles of border and you factor in days off, annual leave, sick leave, you're actually, you know, left with about 3 or 4 agents on duty at a given shift.

Then they're responsible for all of that border and responding to all those sensor activations, whether they're ATS towers—or AST towers, BuckEye game cameras, and then, of course, the remote video surveillance systems.

Mr. BISHOP. By the way, if you're able to acquire targets and go apprehend people, then they get processed and released into the country. That's another issue.

I yield back.

Mr. HIGGINS. The gentleman yields.

I now recognize the Ranking Member of the Subcommittee on Oversight, the gentleman from Maryland, Mr. Ivey, for his questioning.

Mr. IVEY. Thank you, Mr. Chairman.

Mr. Landrum, let me pick up where Chairman Bishop left off with respect to responding to these drone incursions. I suppose they don't actually necessarily need to cross the border just for reconnaissance. They could be on the other side of the border and still, you know, depending on whatever camera capability they have, get whatever information they need without crossing the line.

But let me ask you this: What kind of countermeasures—I think that's what Chairman Bishop was getting at. Do we have the capability to actually respond? My math was like I guess around 30 incursions a day, something like that, with drones that you all were detecting with what you had put up.

Do we have the ability to respond to those in some way, you know, take them down or, you know—I don't know if it has to be an intercept actually, but you mentioned the decoding piece, which apparently they've got the ability to prevent that, but what capabilities do we have to defend ourselves against those kinds of incursions?

Mr. LANDRUM. Congressman, I don't know the current numbers today, but I can tell you that when I retired from Laredo Sector as the chief patrol agent there at that time, I can tell you that at that time we had 2 devices that we could utilize to cover 177 miles. Each device covers about 1 kilometer in each direction, so you can extrapolate the math from that.

It's very difficult to get in the path and to actually mitigate something when you have so few resources to be able to do it. All of that being said, I do think it is super important for this body to understand that getting a complete picture of domain awareness down at the border, so utilizing track, detect, and identify to see every drone at the border, that part is extremely challenging.

Without additional technology to the border in addition—you know, in addition to the RF that's available today, but going to complete RF to detect all drones and radar to detect drones that are not emitting a radiofrequency signal and camera to be able to slew to cue that camera to provide that information to the end-user, all of that is necessary.

Mr. IVEY. Let me follow up on that. So if I'm hearing you right, you have a single device—this is a year-and-a-half ago—that would cover a kilometer each way I think you're saying.

How much would one of those devices cost? What's it called? What's that device called?

Mr. LANDRUM. They're just generally referred to as mitigation devices. It depends company by company.

Mr. IVEY. They're also drones?

Mr. LANDRUM. No, they are not drones.

Mr. IVEY. OK. What are they?

Mr. LANDRUM. They are radiofrequency jamming capabilities.

Mr. IVEY. They have to be devices that are—go up into the air to do that?

Mr. LANDRUM. Their range is about one kilometer, 1.2.

Mr. IVEY. How much does each one of those cost?

Mr. LANDRUM. Rough order of magnitude, you can get them—you could get them from our company as cheap as $50,000 for some mobile devices. Then for some other devices that are available, they could range anywhere from $250,000 up to $800,000 per device.

Mr. IVEY. Let me ask you what's being done—I see I'm running out of time—but what's being done in Israel and Ukraine with respect to intercepting drones?

Mr. LANDRUM. It's still the same technologies of radiofrequency jamming. In some of those cases, they actually utilize—when it comes to mitigation, they'll use what's called kinetic mitigation, which could be something as simple as shooting an AK–47 at the drone that they visually see with their eye.

Mr. IVEY. All right. Last—well, geez, I'm running out of time. But I wanted to actually follow up with Mr. Berteau about the procurement process, because I've heard variations of this with respect to other types of technology, and how to accelerate it.

Because especially in the instance where you have long-term contracts that are, say, 3 years or 5 years or something along those lines. While that contract is running, someone develops a new technology that could actually perform that function better, but they've run into trouble convincing it could be the Department of Defense, I don't mean to pick on them, but whatever the Government agency is, to terminate the contract or do something in order to integrate the new technology and use that.

Has that been your experience, and are there ways to try and address that so we can integrate the new technology that's available?

Then a variation of that, way back in the day on the software piece when the Government was having trouble with that, they went with off the shelf. I think it was GAO or something that did it.

Is there a variation of that where, you know, we've got commercially available in this instance drones—I guess this is a list of commercial companies that are making drones. I'm not sure. But is there a variation of that where we could just—the Government becomes instead of a procurement through the RFP process, which takes forever, as you pointed out, we just do more of an off-the-shelf approach to purchasing these drones or countermeasures?

Mr. BERTEAU. First of all, Ranking Member Ivey, it is a very common problem that a contract in the realm of technology development can become obsolete pretty quickly. That's not the fault of anybody, but it is an actual result of you tend to buy under contract that which you bought before.

The starting point of any renewal contract is basically the old contract that you had in place. So it takes a lot of effort for the

Government to do kind-of the market research to say, what can we do beyond that?

There's 3 things you can do to help fix that. No. 1 is better market research, and we've urged the Government to do that market research not only before the solicitation, before the request goes out for bids, but as they're evaluating the bid.

So, you know, a year after you develop the solicitation, you're evaluating these bids, take a look at what the market can do now, not what it could do 2 years ago when you did your market research. So that's the first thing.

The second thing is actually, as I mentioned earlier, focus on the outcomes and the results you want. If you write that into your contract, it's a lot easier to modify the contract to get what you need as technology evolves rather than have to scrap it and start all over again.

Mr. IVEY. Give me third.

Mr. BERTEAU. The third thing is you need the support of the leadership of the agency to be able to do that. When I mentioned the Joint Rapid Acquisition Council in DOD, it had the strong support of the Secretary of Defense. It had all the people in the room who could waive whatever regulations they needed to waive so you could get that. You can't do that for everything, but you can do it for the most important things.

Mr. IVEY. Well, let me thank the Chair for his indulgence in allowing me to run over. I would ask, as you've offered, for you to provide additional written information about how we can go about integrating that approach. Thank you.

Mr. BERTEAU. We'll be happy to do that, sir. Thank you.

Mr. HIGGINS. The gentleman yields.

I knew not to interrupt Mr. Berteau, because he's married to a Louisiana woman. I don't want to get fussed at.

The Chair recognizes my colleague, my friend Ms. Greene, the gentlelady, for her 5 minutes of questioning.

Ms. GREENE. Thank you, Mr. Chairman. Thank you for being here today.

Fentanyl is the No. 1 killer of Americans between the ages of 18 to 45. It kills approximately 300 Americans every single day. Fentanyl doesn't discriminate based on whether we're Republicans or Democrats, our race, our gender. No identity. Fentanyl doesn't care. It kills people.

Since Joe Biden has taken office, we've seen record amounts of fentanyl pour into our communities from the Southern Border. According to Georgia Narcotics Association, approximately 7 out of 10 pills on the streets are laced with fentanyl, coming across the Southern Border.

In counties throughout my district, in Georgia's 14th District, from—ever since 2020, fentanyl-involved deaths have increased over 350 percent. It's highly prevalent.

Since Joe Biden took office, approximately 62,000 pounds of fentanyl have been seized at the border, yet Federal officials estimate that they are only able to seize 5 to 10 percent of all fentanyl smuggled across the Southern Border.

I'd like to ask each of you about this, because this is Americans being murdered right here at home. We're talking about technology and our Government is spending a lot of money on technology, but where do you believe our border security technology systems are failing so much so that we can only seize 5 to 10 percent of fentanyl smuggled across the Southern Border? I'll start with you, Sheriff.

Sheriff CLEVELAND. Howdy, ma'am. So I can speak to Terrell County. We haven't had a marijuana seizure in about 5 years. The reason we haven't had a marijuana seizure or any other narcotic seizure—and I was the patrol agent in charge at my station for the last 11 years before taking over as sheriff—is because we used to have airplanes that would fly to the border. They would land short of the border, and they'd have radar fades where they'd fall off radar.

AMOC, Air and Marine Operations Center out in Riverside, California, would provide us those GPS coordinates of those radar fades. We would communicate, my station, with the government of Mexico in Ciudad Acuna, and they would send out the Mexican military to either destroy clandestine air strips or seize that marijuana.

So in my county, we have not had any of the fentanyl seizures. But I will tell you that I've spoke at many fentanyl events, and I'm actually flying back into the District of Columbia Friday to speak at the Lost Voices of Fentanyl here on the monument—or, I'm sorry, on the Mall at the monument.

You're right. Fentanyl is killing hundreds of thousands of Americans and China is able to do it without firing a single bullet.

When we—we look at the left. The left is going to tell us that it's coming between—or at the ports. The right is going to tell us it is coming in between the ports of entry. But the honest thing is is that we still have a porous border and it's able to come through.

Ms. GREENE. Thank you, Sheriff.

Mr. Landrum.

Mr. LANDRUM. I would echo everything that Sheriff Cleveland said there. I mean, all of that is true. In my personal experience, in the State of Arizona, I've overseen men and women, Border Patrol agents there that have seized hundreds of pounds of fentanyl. So I've seen it first-hand in my experience there.

In my experience in Texas, I have not seen it in my experience in Texas. So I can't make the same claim that I can when I worked in Arizona.

All of that being said, I completely agree that this is being done, these precursors that are being sent are being done with the full intent from China to actually do that. It is negatively impacting our country to the tune of 100,000 deaths a year, plus or minus in there. That is huge numbers. You can definitely relate it to an act of war.

Ms. GREENE. Thank you.

Mr. Berteau? Did I say that right?

Mr. BERTEAU. Thank you. So I go back a ways in the Government. Back 35 years ago, I actually was the oversight for the DOD role in the counter-drug mission. Nobody heard of fentanyl at that point, right?

But the problems are remarkably similar. There were 3 things. No. 1 is we had trouble detecting. We couldn't tell what was coming in.

No. 2 is, as soon as we closed off one point of egress, they'd find another one. We closed off the Southern Border, they'd come off the California coast. We'd close off the California coast, they'd come in through Vancouver. I suspect that's still at work today, although I'm not up on the day-to-day piece.

No. 3 is the consumption at the other end, right? Because the big problem with the war on drugs, as Mr. Correa mentioned, is we're the market. Now, unfortunately, in those days we had a conscious market that knew what they were buying. Now we have people who have no idea what they're doing.

So I think there are a couple of technical solutions to this. They're probably pretty expensive. I don't—I'm not a technology person, right, but I can try to translate that.

I think it comes into the fact of how do we increase our ability to detect, right? Whether it's 10 percent that we're catching or 20 percent, we'll never be 100 percent but we ought to increase this.

The fourth piece—and I think this is the first time it's been mentioned up here—is the role of China in all of this. I don't think we can ignore the fact that the drone technology is coming out of China. The drug technology is coming from China.

So somewhere you have to get back and interdict at the source as well as at the receiving end, I think. None of those are easy. They're hard to do. They're technically hard to do.

I would certainly want to focus the efforts of this committee on getting the technology to be able to increase our ability to detect, because you can't intercept unless you can detect.

Ms. GREENE. Thank you. I agree with you. We also have to hold the Mexican cartels accountable, because they're the ones smuggling it in the country so—but I definitely agree.

I'm out of time. Thank you, Mr. Chairman.

Mr. HIGGINS. The gentlelady yields.

The gentleman from Mississippi, Mr. Ezell, is recognized for 5 minutes of questions.

Mr. EZELL. Thank you, Mr. Chairman. Thank you, everybody. Thank you, all our witnesses, for being here today.

You can pick almost any spot on the map in the United States and find an example of a border crisis. Every State is now a border State. As a former sheriff, I know this disaster does not just affect a single community. The physical and emotional toll our men and women of law enforcement responding to this disaster is also another cost that can be placed directly on this administration.

We must be doing more to support our first responders. I'm completely supportive of trying to identify easier, better, and safer tools for our law enforcement officers, including their ability to share information.

This is why, with my colleague, Mr. Ivey and I introduced H.R. 8654, the Streamlining Law Enforcement Information Sharing Act. Congress should be finding ways to improve the effectiveness and efficiency of Federal programs intended to help law enforcement collect relevant information from Federal agencies to State and local governments.

Today's discussion focuses on a new technology that can also improve officers' ability to protect our American citizens, but I want to make sure we do so in a way that does not compromise private citizens' data or information.

Sheriff Cleveland, thank you so much for your service, and thank you for being here today. Can you talk a little bit about how advancing technologies and information-sharing platforms enhance your ability to coordinate across agencies and jurisdictions?

Sheriff CLEVELAND. Well, again, having been a Border Patrol agent in my home county, you know, we're pretty well integrated in information sharing there. It's nothing that I've done. It's something that the State of Texas, U.S. Border Patrol, and our county levels along the border and I'd probably say that all along the U.S.-Mexico border just because of the border security issue going back decades. We're pretty well integrated in that manner.

But I would like to mention something I didn't mention in my opening remarks is networking. Something that we've done different in our portion of Texas, and it goes on down the border, is using the same apps to communicate.

We may have a vehicle that comes in my county, and we may see it for a while, suspect it of being there for, you know, reason to smuggle. Then we'll get on our chat group and send it on down the line.

We've had many, many cases of successful interdictions of illegal alien smuggling loads 6, 7 counties down the road, 300 miles down the road right close to San Antonio. So I do agree with what you said, but I do believe we're pretty well integrated along the border at the Federal, State, and local level.

Mr. EZELL. Very good. We know that AI drone systems and similar tools are helpful aids to our law enforcement, but ultimately, a successful operation still comes down to a well-funded, trained, and highly supported, and our personnel.

Do you agree the human aspect is still clearly the most effective factor to achieve your Department's mission as technology advances?

Sheriff CLEVELAND. Most certainly. As I mentioned earlier as well, you know, you can have so much technology detects so much, and if you don't have the manpower to go out and actually put the handcuffs on the bad guy then it's going to be useless.

Mr. EZELL. Very good. I know you are an end-user of the border technology. In your experience, what types of performance metrics are important for us to consider?

Sheriff CLEVELAND. Well, at the local level, mine is my community, you know, am I able to respond to all the incidents that go on. As I mentioned earlier, we don't have a crime problem. We have a border security problem.

I actually have a guest with me here, Mr. Rattly. He's a retired Air Force colonel. He's a landowner down in my county and he spends part of his time up here in Washington, DC, where he has his home.

A few months back, his property was actually broken into. Fortunately, he had a camera system. He was up here in Washington when it happened, and the—he witnessed it happening. He called me immediately.

The hardest thing I can tell a landowner or a citizen in my county—and I've had to do it as both patrol agent in charge at the Border Patrol station and the sheriff—is I don't have anybody to send right now. That was my response to him at that moment.

Mr. EZELL. Oh, my goodness.

Sheriff CLEVELAND. However, he called the neighboring Border Patrol station, the Comstock Station, and they actually had somebody in the area who was able to respond right away. They were able to catch the subject in his house, and then we were able to take custody of that individual to prosecute him.

But there's many examples of similar incidences. So, you know, again, keeping my community safe is going to be my metric in how we assist the United States Border Patrol.

Mr. EZELL. That's, you know, my focus, as a former law enforcement officer like yourself, is manpower. Taking care of the troops, getting them what they need so they can operate and do their job.

So I'm out of time. Thank you all for being here today.

Mr. Chairman, I yield back.

Mr. HIGGINS. The sheriff yields.

The gentleman from Alabama, Mr. Strong, is recognized for 5 minutes for questions.

Mr. STRONG. Thank you, Chairman Higgins, Ranking Member Correa. Thank each of you for being here today.

I don't have to tell you how important cutting-edge technology is for our law enforcement, particularly as they carry out their mission at our borders.

As technology continues to develop for those who wish to do good, so too do the capabilities that those that wish to harm the United States of America. As we have discussed today, we have seen how cartels have, you know, taken drones to carry out illegal activities, including transporting weaponized payloads, conducting surveillance and carrying out attacks on domestic critical infrastructure.

It is my understanding for every drone flown by border security, the Mexican cartel is flying 17 drones. We have technology to drop these drones, block these drones, intercept these drones and do forensics on them. We're already doing this in Israel and the Ukraine is my understanding.

We must have a robust counter-UAS program and capabilities to ensure we are able to meet these threats head-on. Data shows the Mexican cartel are flying drones greater than 30 miles into U.S. air space, landing and offloading drugs on U.S. soil, fentanyl, heroin, cocaine, marijuana, and the list continues.

Mr. Landrum, could you describe some of the challenges with detecting drones entering U.S. air space and how counter-UAS technologies can improve the situational awareness within low-altitude air space at the border?

Mr. LANDRUM. Yes, Congressman. Thank you for the opportunity and the question. When it comes to detecting the drones that are in the air space, it is very easy to detect a DJI drone, because that end-user agrees, through the end-user license agrees to actually transmit that information, which is also very similar to remote ID, which came into effect earlier this year.

Receiving that signal also gives you information such as height, altitude, direction of travel, speed, you know, where it's actually at to actually locate it on a map to be able to do something about it. That is—that in itself is a very challenging process to be able to do that.

To be able to detect all the other non-DJI drones, which in my opening statement I describe as the other 16 manufacturers out there, to detect those others it takes more than just that. It takes direction finding with radiofrequency plus radar plus camera to be able to do that.

In the example in the Laredo demo, where we brought that equipment down there to demonstrate that for CBP over the course of this year, what that did is that exposed the other 29 percent of drones that they were not seeing in that 5-mile stretch.

Mr. STRONG. Thank you. Some of those drones are much smaller than traditional aircraft that would show up on radar. How does this complicate detecting and preventing drone incursion?

Mr. LANDRUM. It is extremely difficult the smaller the device actually becomes. When it comes to the sensor fusion, being able to put something that is found either by radiofrequency or by radar on camera, that is very difficult to accomplish that. It's not insurmountable. We do it as a company, but it is a very expensive process to be able to do it.

Mr. STRONG. Thank you. At least 4 different Executive branch departments—DHS, DOJ, Defense, and Energy—have statutory authority to use counter-UAS technologies, leading to overlap in who can respond to drones near-sensitive sites and critical infrastructure.

In your time in both Government and the private sector, have you ever encountered a delay in response time to a UAS incident because of institutional roadblocks such as overlapping jurisdictions?

Mr. LANDRUM. The only delay was initially in getting 124, an authority that—in my personal experience. So, you know, going back to the 2017–18 time frame, getting that operations plan in place and getting that actually approved. So there was a little delay there.

Now the only thing that would delay that particular response is the lack of equipment or the lack of knowledge that a drone is flying in the air space.

Mr. STRONG. Thank you. Following up on the same vein, would you agree that a dedicated counter-UAS training center for authorized law enforcement and personnel would be valuable?

Mr. LANDRUM. Yes, sir, that would be very valuable.

Mr. STRONG. Thank you. I agree, and that's why I'm working to do just that. Let's create a dedicated counter-UAS training center for authorized law enforcement, train them effectively, and let's take care of business and protect the American people.

Mr. Chairman, I yield back.

Mr. HIGGINS. The gentleman yields.

The gentleman from Arizona, Mr. Crane, is recognized for 5 minutes for questioning.

Mr. CRANE. Thank you, Mr. Chairman, for holding this important hearing today. Thank you to the panel for showing up and trying to educate us and help us understand this problem better.

Sheriff, I want to say thank you for your service, and I want to start with you.

Obviously, we're talking about technology. We're talking about drone, anti-drone technology. As somebody who's been in the field for a long time and supervised others in the field, Sheriff, isn't it true that you can have all the technology in the world, but if your policies don't support the men and women that are designated to protect the homeland, it really doesn't matter?

Sheriff CLEVELAND. Yes, sir, I'd have to agree with that.

Mr. CRANE. Would you agree with the fact that this country, we have a massive amount of debt?

Sheriff CLEVELAND. I sure do.

Mr. CRANE. Yes. The reason I bring that up is because I think everybody that's in here, everybody in here is all about trying to stop these drones and counter the technologies that we see coming into the homeland and making our communities, our families, our States a lot more vulnerable and a lot less safe.

But my issue is, is that this administration, unfortunately, has put policies in place that are completely swamping and overwhelming not only Border Patrol but you guys as well. Would you say that's correct, Sheriff?

Sheriff CLEVELAND. We have definitely—and you missed my opening remarks. We have definitely seen a significant increase in my county of illegal alien apprehensions and got-aways to the tune—at the highest watermark, we had a 417 percent increase in fiscal year 2022 compared to fiscal year 2020, and that was with apprehensions, and a 467 percent increase in got-aways that same year.

Mr. CRANE. What about you, Mr. Landrum? Do you agree with that point, that you can have all the technology in the world, but if you don't have leadership that's actually dedicated to stopping the flow of whatever it is, whether it be drones, drugs, MS–13 gang members, terrorists, suspected terrorists on the watch list coming through the Southern Border, it really doesn't matter?

Mr. LANDRUM. You absolutely need the leadership and the authorization to do it. Something that we as a company and me personally as a retired agent support is the expansion of those authorities, the 124n authorities, to be able to do these activities to State, local, Tribal, and territorial law enforcement officers and agents.

Mr. CRANE. Yes, absolutely, because at the end of the day there's no golden conex box up here. I mean, well, we kind-of act like there is. We just charge it to the Americans' people's credit card and to their kids' credit card and their grandkids' credit card as we run up the national debt.

But the bottom line is, like I'm saying, if you don't have policies that actually reflect a desire to stop the flow of what's coming over that Southern Border, it really doesn't matter, because our law enforcement, our Border Patrol, their budgets are just completely overwhelmed with everything coming over that Southern Border.

I know, Mr. Berteau—is that how you say it? You were talking about I think 4 things that Congress can do. Can you repeat that list real quick, sir?

Mr. BERTEAU. Let me make sure I get it right by actually looking at my notes. Thank you.

So, first of all, we think that DHS can focus its contract requirements on results, right, rather than on input. So you're actually focused on what you want the contract to be able—the results of that contract to be able to help, in this case Border Patrol agents, for example, to be able to do. What can they do differently?

Focusing on results allows you to get past a lot of the problems in the contracting process, including, as we discussed earlier, what happens if technology evolves? Well, if you've got the results built into the contract, you can evolve the contract a little bit. So that's No. 1.

Second is resources, because resources drive strategy way more than strategy drives resources. So we urge the Congress to actually give DHS its appropriations on time rather than 6 or 7 months into the fiscal year so CBP has the money and a whole year to buy it. You'll get the results a lot sooner.

Third is, in fact, to hold their feet to the fire in terms of how long contracts take. Get the data. Get DHS to be reporting that. Get them to give you an annual report that says, here's how long our contracts take. Until you're measuring something, you're not going to be able to take the steps to actually reduce that something.

The third is—oh, the fourth is, you got to train the workers to do it, because, as you point out, if the workers can't handle it and deal with it, it's going to be a problem, not a solution.

Mr. CRANE. Thank you, sir.

Mr. Chairman, I yield back.

Mr. HIGGINS. The gentleman yields.

It looks like we have no further questions for the panelists today. I have some data to submit to each of you in writing, because it was brought up during questioning regarding the budget and the needs for resources.

So I'm going to share with you in writing, all of you but Mr. Landrum in particular, how much the budget has increased for the Department of Homeland Security over the last 4 years.

So I thank the witnesses for their testimony today and the Members for their questions. Members of the subcommittees may have additional questions for the witnesses.

Mr. Chairman, do you have any further questions?

Mr. BISHOP. No, Mr. Chairman.

Mr. HIGGINS. May have additional questions for the witnesses, and we would ask for the witnesses to respond to these in writing. Pursuant to committee rule VII(D), the hearing record will be held open for 10 days.

Without objection, the subcommittees stand adjourned.

[Whereupon, at 3:45 p.m., the subcommittee was adjourned.]

APPENDIX I

QUESTIONS FROM HONORABLE DELIA C. RAMIREZ FOR CARL LANDRUM

Question 1. How does your company separate decisions about the tech you develop and sell to combat drug and arms smuggling from decisions about the tech you develop and sell to help CBP to facilitate humane and effective processing of immigrants and asylum seekers?

Answer. Dedrone's stated mission is: "To protect against malicious drones while enabling good drones to fly".

Our current focus working with CBP is on countering the usage of drones by transnational criminal organizations (TCOs) along our borders, which includes illicit and deadly activities such as drug and arms smuggling. Looking to the future, Dedrone offers technology that could assist CBP in the first stages of supporting immigrants and asylum seekers. DedroneBeyond enables first responders to safely and effectively navigate their drones Beyond Visual Line of Sight (BVLOS) to enable an agency like CBP, using drones, to more quickly and appropriately respond to migrants and their needs in their first moments in the United States.

Question 2. As we talk about providing CBP with more technology and increasing its collaboration with the private sector, we must consider how CBP and companies can ensure individuals' civil rights and civil liberties are protected. How does your company take steps to protect sensitive Government information, including personally identifiable information?

Answer. Dedrone is committed to maintaining a strong cyber and information security posture, aligning its practices with recognized standards such as ISO 27001 and NIST 800–53. Our approach ensures that we implement comprehensive security controls across our entire technical stack, including software, hardware, and protocols. This allows for the safeguarding of data integrity, confidentiality, and availability. By directly aligning to these stringent standards, we continually assess and improve our security measures to protect against evolving threats.

Specific to personal identifiable information (PII) and providing solutions for CBP, Dedrone does not utilize any PII except that of the user (ie: CBP employees) in the form of work emails and telephone numbers.

QUESTIONS FROM RANKING MEMBER GLENN IVEY FOR DAVID J. BERTEAU

Question 1a. The men and women of U.S. Customs and Border Protection (CBP) are the greatest asset we have in securing the border and keeping Americans safe. Yet, we are facing significant shortages in front-line CBP personnel—more than 5,000 officers and agents—and this may worsen with increasing retirements. Technology can help bridge this gap.

As we deploy new technology, it's the men and women who are on the ground every day who will operate this technology and turn information provided by the technology into apprehensions, drug seizures, and rescues.

How can CBP ensure that the technology it deploys will help bridge the gap in personnel and best support officers and agents in the field?

Answer. Many emerging technologies have the capabilities to reduce work loads on current personnel and create efficiencies which were not possible just a decade ago. The keys are to evaluate these technologies and pursue them with urgency but to do so with the user in mind. As I noted in my statement submitted for the hearing, CBP needs to train to use new technology.

We all know how hard it is to adapt to an upgrade or an innovation in something that we are used to, whether it is using a new cell phone, the latest version of the operating system of a laptop, or the features and controls of a new car. This same dynamic exists when any agency or component incorporates new technology and innovation into existing operations.

To offset this natural occurrence, DHS components could plan for and fund the time, the resources, and the capacity and capability to train the workforce to take advantage of new technology. Contractors can help develop and provide that training more rapidly and broadly.

However, it takes more than training. Technology improvements are, by definition, fast-moving, which means that it is important for requirements to take into account the ability of the workers to use it. Such requirements take more than technical expertise and market research; they need to have user involvement from the early stages of the acquisition process. This committee could encourage DHS and CBP to increase such user involvement in defining requirements, in the research that helps identify what is available in the current and future marketplace, and in the evaluation of proposals. Such user involvement can take more time up front but can pay off in implementation.

Question 1b. When developing new technology for CBP, how should companies incorporate feedback and input from field personnel?

Answer. In my experience, feedback from field personnel does not automatically flow to contractors. Too often, those who are setting the acquisition requirements and evaluating bids are not well-connected to the actual workers who will use new technology to accomplish their missions. The employees in the field know the pain points and the specific problems which need to be dealt with. Their input is critical to acquiring the right technological solutions. Contractors seek to offset this lack of connection by doing their own research into the needs of the user. This ensures technological solutions which actually address the problem and are implementable when employed by the end-user. Acquisition programs which fail to seek and assess such input create the risk of failing to address the real needs of field personnel.

Question 2. CBP invests billions in technology and assets; yet purchases often cost more and take longer than CBP expects. Such delays can result in technology becoming outdated before it becomes operational. How can CBP better ensure that it can acquire the most up-to-date technology in a timely manner?

Answer. The Federal Government's cycle of acquisition, from developing requirements through obtaining resources through Congress to soliciting, evaluating, and awarding contracts is simply longer than the cycle of developing new technology. My statement for the record cites several steps DHS and CBP could take to mess these cycles better.

DHS components can better ensure that they are acquiring useful technology and systems and process improvements in a timely way by:

- Focusing requirements, both for contracts and for operations, on results and outcomes,
- Making those requirements publicly available early, so that companies can work to develop technology to meet them,
- Updating those requirements often to reflect newly-available innovation,
- Developing and making publicly available a long-term (e.g., 5-year) investment plan and updating that plan regularly,
- Expanding the frequency and the depth of communications with industry,
- Encouraging both existing and potentially new contractors to offer solutions and giving feedback to those offerings (companies respond to CBP and DHS requests for information but rarely get feedback on their responses),
- Reducing the time between soliciting a contract and awarding it (Congress can help this by requiring DHS components to report these times every year and explain why they are not shorter).

QUESTIONS FROM HONORABLE DELIA C. RAMIREZ FOR DAVID J. BERTEAU

Question 1a. The technology and protocols we use to stop smuggled contraband are not the appropriate technology and protocols to use to address people seeking safety and stability. What would it take to have discussions about technology and border security that do not conflate and talk about people and illicit goods as if they are the same?

Answer. Managing the cross-border movement of people and of goods are indeed quite different, but they share a common dilemma. How can the Federal Government operate in a way that encourages and supports the appropriate flow of people and goods while inhibiting improper or illicit movement of both. In my experience, actors who encourage and/or benefit from illicit trafficking of both people and goods do not differentiate between the two; the paths and operating mechanisms are inextricably intertwined.

That said, and as highlighted in my written testimony for the July 9, 2024, hearing on "Smart Investments: Technology's Role in a Multi-Layered Border Security Strategy", private sector-provided technology can support a multi-layered U.S. border strategy that separates people and goods at various stages of the movement process. For example, the private sector can support U.S. Federal agencies with:

- Intelligence capabilities before individuals (whether immigrants, asylum seekers, or traffickers in illicit goods) arrive at any U.S. border;
- Detection, identification, interception, etc. technologies, both at and away from authorized ports of entry. Such capabilities can support Federal missions to interdict controlled substances or other unwanted materiel arriving in small packages or in containers (or via drones), as well as tracking people;
- Responsible detention, housing, and medical care, and other services that can and should be provided to individuals after they cross into U.S. sovereign territory; and
- Case processing, reduction, and backlog management for individuals who have entered the United States.

This broader, multi-layered approach would involve U.S. Customs and Border Protection, as well as other relevant agencies and components of the Federal Government, State and local government entities (e.g., law enforcement), and other nations. In all of these interactions, a multi-layered strategy could incorporate new technology and innovation in products, systems, and processes and lead to better success across the broad definition of "border security."

Question 1b. As we talk about providing CBP with more technology and increasing its collaboration with the private sector, we must consider how CBP and companies can ensure individuals' civil rights and civil liberties are protected. How do your companies take steps to protect sensitive Government information, including personally identifiable information?

Answer. Private-sector companies who perform work under Federal Government contracts in support of border security and immigration missions, agree to and abide by specific requirements and exacting standards. These requirements and standards are specified in the Federal Government's requests for proposals (RFPs) and in the contracts that are issued to companies responding to those RFPs. CBP, DHS, and the Federal Government can protect rights and liberties by ensuring that such protections are included in contracts and by evaluating and awarding to companies that have a track record of success in complying with such requirements.

In most if not all contracts, for example, safeguarding sensitive Government information, including but not limited to personally identifiable information, is among those requirements, and Government contractors take these obligations very seriously.

However, it takes time and money to comply with such obligations, and the Federal Government must include coverage of such costs in their solicitations and in the contracts subsequently awarded and implemented.

In addition, Government contractors' systems and processes are subject to regular and unscheduled audits or other reviews by Federal agencies.

QUESTIONS FROM HONORABLE YVETTE D. CLARKE FOR DAVID J. BERTEAU

Question 1. How do interruptions in Government funding—including Government shutdowns, operating under Continuing Resolutions, and late budgets—impact agencies and their ability to make procurements and acquisitions?

Answer. Representatives of the Government contractor community—including but not limited to PSC—have long argued that funding uncertainties significantly harm every Government agency's ability to plan and execute acquisitions. This harm occurs even if a Government shutdown is avoided, as thousands of Government officials divert their attention to planning for a potential upcoming lapse in appropriations, even if Congress subsequently delays that lapse for additional weeks or months.

The question has a flip side, which is to ask what would be the benefits of Congress enacting full-year appropriations on time, so that agencies have a full year to execute the programs and funding authorized and appropriated by Congress. Agencies have the time to research emerging technology, solicit bids, and award contracts. Work can spread across 12 months instead of being crammed into half a year. Benefits accrue sooner, technology is deployed faster, field agents can train earlier. Everyone wins.

Funding uncertainty and interruptions also cause direct harm to our Nation's industrial base, its work force, and its ability to support critical Government missions. They are particularly bad for many thousands of small and mid-sized businesses.

As stated in my May 16, 2019, written testimony at a House Committee on Oversight and Reform hearing on "Government Shutdowns: Contract Killers",

"The contractor community plays many vital roles in assisting the Government to meet the needs of the American people. Contractor contributions are necessary to maintaining Government operations. Many of the capabilities that contractors provide do not exist, or are insufficiently available, within the Government, and contractors can expand or adjust their capacity to meet changing mission needs more quickly than their Federal counterparts. Contractors bring innovation and solutions from a strong, diversified national interest business base to support current and emerging requirements for every agency of the Government.

"Like the Federal employees they work beside, contract employees show up every day to do jobs that are vital to the Government's ability to achieve its missions and functions. They are motivated by the same goals of public service and safety as their Government counterparts. All of us—Federal workers, contractors, and the American people—deserve Government efforts to avoid any lapse in appropriations. Failing that, if there is a future lapse in appropriations for part or the whole of the Federal Government, we need a better system to communicate to all stakeholders and to manage the business of Government.

"More specifically, and as noted in a September 23, 2023, PSC letter to Congressional leaders, Federal Government funding disruptions—particularly those from a Government shutdown—result in work stoppages from Federal agencies, leading to layoffs of workers and financial instability for all companies that support Federal missions. These disruptions in turn produce cascading effects on those missions—from military readiness and America's ability to deter adversaries . . . to systems modernization and the provision of fast, effective customer service to the American people.

"As you can imagine, shutdowns are worse than continuing resolutions. As noted in my 2019 testimony cited above, shutdowns cause remarkable harm to America's combined Federal workforce (specifically contractor and civilian personnel), the companies' financial well-being, and productivity.

"However, the negative impact of a CR on Government contractors and mission success also remains acute. CRs delay programs and defer new starts, which dampens innovation and creates unpredictable cash-flow situations for companies; this is disproportionately hard on small businesses.

"PSC has long advocated for several practical steps to mitigate the impact of funding disruptions, whether shutdowns, CRs, or other delays. Examples of these steps include: (1) enact full-year appropriations bills prior to the start of each fiscal year; (2) trigger automatic Continuing Resolutions before a lapse in appropriations; (3) prioritize spending agreements that will set appropriate budget caps for fiscal years so that budget levels are known in advance; (4) provide parity for contractors regarding 'back pay' compensation similar to what is provided for Federal military and civilians personnel; (5) enhance data collection requirements so the Government can document lessons learned in planning for and implementing a shutdown, as well as resuming activities following a shutdown (as recommended in an October 2014 Government Accountability Office report, '2013 Government Shutdown: Three Departments Reported Varying Degrees of Impacts on Operations, Grants, and Contracts'; (6) improve shutdown-related communication and guidance—from the Office of Management and Budget to the agencies and from the agencies to their contracting partners—as it pertains to contract administration so that the Federal contracting community within the Government and companies alike can level-set expectations. My 2019 testimony cited above expands on each of these recommendations and includes additional suggestions to help support Government acquisition in the face of funding uncertainties."

Question 2a. Artificial Intelligence (AI) should be utilized as a tool—not a substitute for human decision makers—to enhance our operations at the border to ensure a safe, orderly, and humane immigration process. Yet, biases that have been identified with AI as it relates to race, ethnicity, and gender, could cause unnecessary harm to individuals entering this country legally or seeking asylum.

What needs to be done to ensure bias within AI does not discriminate against or reduce people's ability to participate in our economy and society?

Question 2b. What can be done to encourage private industry to continue progress on research and standards that will reduce bias in AI?

Answer. Artificial-Intelligence-related challenges are a particularly tough aspect of new technology. As Americans become more familiar with, and use, AI in their daily lives and as the U.S. Government explores ways to leverage AI to support the full range of Federal missions, it is important to address a wide range of issues. One such issue is the various biases that can accompany AI-enabled technologies and how to identify and mitigate potentially adverse impacts on individuals' rights and freedoms as well as on the efficacy of the results.

The Professional Services Council (PSC) has repeatedly stated that adequate safeguards and guardrails must be in place when Federal agencies solicit, procure, and use commercially-developed AI products and services within the Federal environment. This is especially true when such use could directly impact the American taxpayer and communities (particularly underserved communities).

In general, the Government contracting industry supports safeguards and guardrails, where appropriate, to mitigate risks of bias, while also seeking to encourage innovations that can emerge from development and use of AI technologies. From an acquisition perspective, PSC has encouraged Federal agencies to work with industry to incorporate safeguards and guardrail requirements at the beginning of the acquisition life cycle. Agencies need to communicate with commercial vendors on how best to mitigate against bias before the delivery of goods and services that could have profound impacts on the American taxpayer.

Executive Order 14110 on the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" and Office of Management and Budget (OMB) M–24–10 Memo "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" instructs agencies to advance the management and innovation of AI while mitigating risks related to AI use in the Federal Government, especially concerning public rights and safety. Core to this, from our perspective, is data—from data provenance to how data is collected, stored, used/analyzed to who has access to data in the Federal environment.

PSC has previously recommended the following actions to mitigate against bias, discrimination, and impacts from AI hallucinations:

- *Harmonizing Federal AI guidance*.—As AI and generative AI (GenAI) is in its infancy, there is a unique opportunity to establish order and harmony now in how it should be adopted before its wide-spread, disparate use across the Federal Government complicates such efforts. PSC believes that this type of consistency will help commercial vendors work with disparate agencies and support innovation Government-wide through similar requirements and compliance regimes. PSC recommends that OMB Memo M–24–10 together with the NIST AI RMF Guidance should supersede agency principles and guidance and that coordination between OMB and Federal agencies should occur to reconcile conflicting guidance.
- *Keeping humans in the loop*.—AI, much like humans, is prone to errors. Though AI tends to make fewer mistakes overall, the nature of these errors differs significantly from those typically made by humans. Since AI risk factors can only be mitigated and not completely eliminated, PSC urges Federal policy makers and regulators to consider what threshold need to be met for AI and GenAI to be procured and adopted from a mission perspective (i.e., the appropriate role of humans to monitor, supervise, and support operations alongside AI and GenAI in the Federal context.)
- *Monitoring human involvement of commercial AI and GenAI*.—Federal agencies should consider incorporating GenAI governance and oversight structures for monitoring purposes. PSC recommends establishing governance protocols that protect proprietary information from unauthorized access or usage (i.e., govern how Federal operators interact with data when using AI and GenAI technologies.) Such governance protocols can establish steps to inform Federal operators on: (1) identifying the provenance of the data; (2) how data should be cleaned and labeled; and (3) who has authority to access and run the data through the model. PSC believes that once these steps are established, they can provide justification for specific prompts taken by the Federal operator and identity errors and where fixes need to occur.
- *Determining appropriate AI Use Cases in the Federal context*.—A December 2023 GAO report highlighted that "Without accurate inventories, the government's management of its use of AI will be hindered by incomplete and inaccurate data." PSC believes the appropriate identification of AI Use Cases and completed inventories will support the appropriate safeguards, guardrails, and use of AI and GenAI in the Federal context and that those completed AI Use Case inventories can support innovation. The inventories can also help each agency assess its AI maturity levels and what AI Use Cases could work for their specific mission challenges.