DETER, DETECT, AND INTERDICT: TECHNOLOGY'S ROLE IN SECURING THE BORDER

HEARING

BEFORE THE

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JULY 25, 2017

Serial No. 115–23

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

27–977 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
JEFF DUNCAN, South Carolina
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
JOHN KATKO, New York
WILL HURD, Texas
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
MIKE GALLAGHER, Wisconsin
CLAY HIGGINS, Louisiana
JOHN H. RUTHERFORD, Florida
THOMAS A. GARRETT, JR., Virginia
BRIAN K. FITZPATRICK, Pennsylvania
RON ESTES, Kansas
BENNIE G. THOMPSON, Mississippi
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California

BRENDAN P. SHIELDS, *Staff Director*
KATHLEEN CROOKS FLYNN, *Deputy General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
HOPE GOINS, *Minority Staff Director*

SUBCOMMITTEE ON BORDER AND MARITIME SECURITY

MARTHA MCSALLY, Arizona, *Chairwoman*

LAMAR SMITH, Texas
MIKE ROGERS, Alabama
JEFF DUNCAN, South Carolina
LOU BARLETTA, Pennsylvania
WILL HURD, Texas
JOHN H. RUTHERFORD, Florida
MICHAEL T. MCCAUL, Texas *(ex officio)*
FILEMON VELA, Texas
CEDRIC L. RICHMOND, Louisiana
J. LUIS CORREA, California
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
BENNIE G. THOMPSON, Mississippi *(ex officio)*

PAUL L. ANSTINE, *Subcommittee Staff Director*
ALISON NORTHROP, *Minority Subcommittee Staff Director/Counsel*

CONTENTS

DETER, DETECT, AND INTERDICT: TECHNOLOGY'S ROLE IN SECURING THE BORDER

Tuesday, July 25, 2017

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:04 a.m., in room HVC–210, Capitol Visitors Center, Hon. Martha McSally (Chairwoman of the subcommittee) presiding.

Present: Representatives McSally, Smith, Hurd, Rutherford, Vela, and Barragán.

Ms. MCSALLY. The Committee on Homeland Security Subcommittee on Border and Maritime Security will come to order. The subcommittee is meeting today to examine the role of technology in the Nation's border security efforts.

I now recognize myself for an opening statement.

Border security is a complicated endeavor because there is no one-size-fits-all solution. Thinking through what it will take to secure the border is the primary responsibility of the three agencies represented by our witnesses today. Border Patrol is our operational force between the ports of entry. CBP's Office of Field Operations' job is to facilitate legitimate trade and travel while keeping a list of drugs and people from entering our country illegally at the ports of entry.

Air and Marine is the supporting element, which provides air and maritime interdiction support and situation awareness for critical operations on the ground. All three of these critical border security components rely heavily on technology to accomplish their mission.

Indeed, technology is a crucial force multiplier, and part of our multi-layered approach of the right mix of infrastructure, personnel, and technology that we have used for at least 20 years now.

Instead of focusing solely on the gadgets and the gizmos and the many repeated failures we have had in the procurement process at CBP, I think it is important to think strategically about the decision-making process.

Those who aim to exploit our border for illicit purposes. Destructing that process by leveraging technology will help Customs and Border Protection better use the allocated funding to secure the border in the long term.

So today I want to take a hard look at the role that technology plays in helping to predict, deter, detect, and finally interdict the illicit activity so prevalent along the Southwest Border.

Deterrence is the ideal goal in the Nation's border security effort, yet it is difficult to measure or accomplish. Discouraging bad actors from ever crossing the border is our best defense. If our security posture is robust, individuals may decide it is not worth the risk to smuggle a load of drugs across the Arizona desert or through a busy port of entry.

Essentially, deterrence is predicated on two things: First the perception that illegal smuggling across the border is a costly endeavor; and second that the likelihood of success is low.

But if we cannot successfully deter illegal behavior by communicating the message that the border as an inhospitable place to conduct illicit cross-border activity, then we have to shift to detection, surveillance, and interdiction.

That is where the role of technology becomes indispensable because of the rugged and remote nature of many parts of the border. Terrain, the prevalence of roads and other infrastructure on both sides of the border, and CBP's security posture in any given area should inform the tools we use to detect, monitor, and surveil the border.

On a consistent basis, these tools are critical for what is commonly referred to as situational awareness, or SA, a basic requirement if the goal is to gain operational control of the Southern Border. Cameras, night vision devices, motion sensors, radar, X-ray devices, and other surveillance equipment have become essential elements of our robust security operations.

These technologies have enhanced agent and officer safety, provided constant monitoring of difficult-to-access areas, and enhanced agent and officer ability to interdict the criminal activity. Aviation assets, such as unmanned aerial vehicles equipped with advanced radar capabilities, have also refined our understanding of the significant threat that exists along the border and helped to reposition and redeploy assets as flows and vulnerabilities shift.

I understand that Border Patrol and CBP Air and Marine continue to pilot tactical UAVs that have the potential to revolutionize the way we conduct border security operations at the field agent level. I look forward to a progress update in light of the additional funds Congress has provided for this particular effort.

A secure border is the outcome that American people demand, regardless of what steps that we all take to get there. With this in mind, Congress has repeatedly asked one consequential question. What will it take to gain this situational awareness and operational control of the Southwest Border?

Up until now, the answers we have received have been limited or unsupported by our acquisition process similar to that of the Defense Department. In short, they have been insufficient. At best, they have been some best guesses.

Congress expects the Border Patrol Office of Field Operations and Air and Marine to be able to quickly identify and justify the technological needs required to secure the border. So far the Border Patrol and Air and Marine operations have been involved in an effort called the Capability Gap Analysis Process or C–GAP.

C–GAP is a scenario-based exercise designed to ferret out tactical weaknesses in our border security defenses and hopefully inform the technological budget process. Putting more technology on the

border will increase our chances of apprehending dangerous individuals and interdicting lethal drugs like heroin and Fentanyl that cause so much death and pain for our fellow American citizens.

Thanks for being here to discuss the many ways in which we can be using technology to secure our Nation's border, and I look forward to the witnesses' testimony.

[The statement of Ms. McSally follows:]

STATEMENT OF CHAIRWOMAN MARTHA MCSALLY

JULY 25, 2017

Border security is a complicated endeavor because there is no one-size-fits-all solution. Thinking through what it will take to secure the border is primary responsibility of the three agencies represented by our witnesses today.

The Border Patrol is our operational force between the ports of entry. CBP's Office of Field Operations job is to facilitate legitimate trade and travel while keeping illicit drugs and people from entering our country illegally at the ports of entry. Air and Marine is a supporting element—which provides air and maritime interdiction support and situational awareness for critical operations on the ground.

All three of these critical border security components rely heavily on technology to accomplish their mission. Indeed, technology is a crucial force multiplier, and part of a multi-layered approach of the "right mix of infrastructure, personnel, and technology," that we have used for at least 20 years.

Instead of focusing solely on the gadgets and gizmos and the many repeated failures of the CBP procurement process, I think it is important to think strategically about the decision-making process of those who aim to exploit our border for illicit purposes.

Disrupting that process by leveraging technology will help Customs and Border Protection better use the allocated funding to secure the border in the long term.

So today, I want to take a hard look at the role that technology plays in helping to predict, deter, detect, and finally to interdict the illicit activity so prevalent along the Southwest Border.

Deterrence is the ideal goal of the Nation's border security effort, yet is difficult to measure or accomplish. Discouraging bad actors from ever crossing the border is the best defense. If our security posture is robust, individuals may decide it's not worth the risk to smuggle a load of drugs across the Arizona desert or through a busy port of entry.

Essentially, deterrence is predicated on two things: First, the perception that illegal smuggling across the border is a costly endeavor; and second, that the likelihood of success is low.

If we cannot successfully deter illegal behavior by communicating the message that the border is an inhospitable place to conduct illicit cross-border activity, then we have to shift into detection, surveillance, and interdiction. That is where the role of technology becomes indispensable because of the rugged and remote nature of many parts of the border.

Terrain, the prevalence of roads and other infrastructure on both sides of the border, and CBP's security posture in any given area should inform the tools used to detect, monitor, and surveil the border.

On a consistent basis, these tools are critical for what is commonly referred to as situational awareness—a basic requirement if the goal is to gain operational control of the border.

Cameras, night vision devices, motion sensors, radar, X-ray devices and other surveillance equipment, have become essential elements of our border security operations.

These technologies have enhanced agent and officer safety; provided constant monitoring of difficult-to-access areas, and enhanced agent and officer ability to interdict criminal activity.

Aviation assets such as Unmanned Aerial Vehicles, equipped with advanced radar capabilities, have also refined our understanding of the significant threat that exists along the border and has helped reposition and redeploy assets as flow and vulnerabilities shift.

I understand that the Border Patrol and CBP Air and Marine continue to pilot tactical UAVs that have the potential to revolutionize the way we conduct border security operations at the field agent level. I look forward to a progress update in light of the additional funds Congress has provided for this effort.

A secure border is the outcome the American people demand—regardless of what steps we take to get there.

With this in mind, Congress has repeatedly asked one consequential question: What will it take to gain situational awareness and operational control of the Southwest Border?

Up until now, the answers we have received have been limited, or unsupported by a requirement process similar to that of the Defense Department. In short, they have been insufficient; at best, they have been guesses.

Congress expects the Border Patrol, the Office of Field Operations, and Air and Marine to be able to quickly identify, and justify, the technological needs required to secure the border.

So far, the Border Patrol and Air and Marine Operations have been involved in an effort called the Capability Gap Analysis Process, or C–GAP. C–GAP is a scenario-based exercise designed to ferret out tactical weaknesses in our border security defenses and hopefully inform the technological budget process.

Putting more technology on the border will increase our chances of apprehending dangerous individuals and interdicting lethal drugs like heroin and fentanyl that cause so much death and pain for our fellow American citizens.

Thank you for being here to discuss the many ways in which we can be using technology to secure our Nation's borders. I look forward to the witness's testimony.

Ms. MCSALLY. The Chair now recognizes the Ranking Member, the substitute Ranking Member, the gentleman from California, Mr. Correa, for opening statement.

Mr. CORREA. Thank you, Madam Chairwoman. I am pleased to join you for today's hearing examining U.S. Customs and Border Protection's efforts to enhance border security with the use of technology.

Ranking Member Vela can't join us today due to some other commitments, so I am happy to step in in his stead. Over the past several years, we have seen technology used to improve situational awareness, enhance security, and to improve legitimate commerce across our borders.

While Secretary Kelly and many lawmakers in Congress talk about the value of technology to better secure our borders, we remain concerned that we are not utilizing technology to its fullest benefits. We know the new Trump administration has prioritized physical barriers over technology to secure the border.

President Trump ran for office with the promise to build a wall to stop undocumented immigrants and to curb drug smuggling. While experts before this committee have told us that a border wall will not accomplish either one of these goals, earlier this month the Appropriations Committee approved $1.6 billion for the construction—or I should say continued construction of that border wall.

While we allocate billions in a border wall that may not work, I am hearing stories of many of our border agents not being able to talk to each other using their existing equipment. I have heard some of these folks tell me that they can see each other 2- to 300 yards away, yet they can't use some of their walkie-talkies. To me that is just a sad testament to the situation we have with reference to existing technology.

With limited resources for technology on the border, it is important that Customs and Border get it right when it comes to procuring, testing, and employing technology along the border. The Department of Homeland Security has for years attempted to deploy various kinds of technology to the borders with mixed results at best.

Identifying, inquiring, and deploying the right mix of border security technology isn't easy, but we got to get it right. A million

here, a million there translates to a billion here and a billion there. Those dollars, we can only spend once. Those are very precious taxpayer dollars.

We know that the flow of border crossers and illicit traffic changes from day-to-day, and our technology and our tactics need to evolve along with those changes. This is another reason, a primary reason why a border wall, in my opinion, is not a solution to our border security challenges. Remember, we have two borders, and we have two oceans.

America's borders are varied as well with different geography, terrain, and climate. Given DHS's poor track record and seemingly unending shift to physical barriers of technology, I remain concerned about our border security and technology deployment.

I would like to hear today CBP justify why a wholesale physical infrastructure plan would be more effective than deploying strategic technological assets along the border. As Secretary Kelly has said here numerous times, the border, rather, we need a multi-layered defense system.

I also hope to hear from our GAO witness today about their examination of CBP's metrics to measure the performance of border technologies and whether DHS's procurement and acquisition management processes are sound or still need to be improved.

Also in light of the mess of acquisition management resources that would be needed to be dedicated to constructing a physical wall, I would like to know how CBP will manage existing technology contracts as it shifts to focus on personnel to man the new wall.

Finally, I hope we can have a frank discussion with our witnesses about how CBP can best position its on-going border security technology programs for success in this environment of scarce resources. I thank the witnesses for joining us here today.

I yield back my time, Madam Chair.

Ms. MCSALLY. The gentleman yields back.

Other Members of the committee are reminded that opening statements may be submitted for the record. We are pleased to be joined today by four distinguished witnesses to discuss this important topic.

Mr. Todd Owen is the executive assistant commissioner for the Office of Field Operations. Prior to becoming executive assistant commissioner, Mr. Owen served in various roles within CBP's Office of Strategic Trade and most recently, as the director of field operations at CBP's Los Angeles field office.

Mr. Scott Luck began his career with the Border Patrol in 1986 and currently serves as the acting deputy chief of the U.S. Border Patrol. Prior to becoming acting deputy chief, Mr. Luck was the Chief of Operations Division for the U.S. Border Patrol.

Dennis J. Michelini serves as the acting executive director of operations for U.S. Customs and Border Protection's Air and Marine Operations Division. Mr. Michelini began his career with CBP in 1995 where he served as an agent and a pilot. Prior to becoming the acting executive of operations, he served as director of the northern region and director of air operation strategy.

Ms. Rebecca Gambler is director of the U.S. Government Accountabilities Office Homeland Security and Justice Team, where

she leads GAO's work on border security, immigration and the Department of Homeland Security's management and transformation.

The witnesses' full written statement will appear in the record.

The Chair now recognizes Mr. Owen for 5 minutes to testify.

STATEMENT OF TODD C. OWEN, EXECUTIVE ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. OWEN. Good morning, Chairwoman McSally, Ranking Member Vela, Mr. Correa, esteemed Members of the subcommittee. Thank you for the opportunity to testify today alongside my colleagues from the U.S. Border Patrol and Air and Marine Operations to discuss the role of CBP's Office of Field Operations in detecting and interdicting illegal drugs and other dangerous materials at our ports of entry.

Before my appointment as the executive assistant commissioner of CBP's Office of Field Operations in February 2015, I served in several relevant roles within CBP, most recently as the director of field operations for the greater Los Angeles area and previously as the executive director over all of CBP's cargo security programs.

I know first-hand how valuable technology is to CBP's ability to detect materials that potentially pose a threat to the United States.

Used in conjunction with CBP's risk-based targeting capabilities and security partnerships, advanced detection technology at our ports of entry is an essential component in our mission to intercept illegal drugs and other dangerous materials before they cross our borders.

Smugglers use a wide variety of tactics and techniques for concealing drugs and other contraband through the ports of entry. CBP officers regularly find drugs concealed on individuals, hidden inside vehicle seat cushions, gas tanks, dashboards, and tires, within packaged food, household goods, and hygiene products, in checked luggage, and in construction materials transported on commercial trucks.

This past weekend, CBP officers in Laredo discovered and seized 147 pounds of cocaine hidden in the gas tank of a commercial bus. While in Nogales, CBP officers intercepted three internal carriers of heroin and methamphetamine. All three U.S. citizen females were traveling together and had entered through the pedestrian lanes.

Yesterday in Brownsville, CBP officers seized 118 pounds of methamphetamine concealed in tires of a passenger vehicle. These are but three real-life examples of the threats that CBP officers address every day.

To counter the full range of concealment techniques, CBP incorporates advanced technology to maintain a robust cargo, commercial conveyance, and vehicle inspection regimes at our ports of entry, including the use of non-intrusive inspection equipment or NII equipment, as well as radiation detection technologies.

NII technologies deployed to our Nation's land, sea, and air ports of entry include large-scale X-ray and gamma-ray imaging systems, as well as a variety of portable and hand-held technologies.

These technological systems enable CBP officers to examine cargo conveyances such as sea containers, commercial trucks, railcars, and privately-owned vehicles for the presence of contraband without physically opening or unloading them.

NII equipment is a force multiplier, which allows CBP to work smarter and faster in detecting contraband while expediting legitimate trade and travel. Detection technology is a critical contributor toward enforcement actions at ports of entry.

In 2016 large-scale NII systems were used to conduct more than 6.5 million examinations resulting in more than 2,600 seizures and over 359,000 pounds of seized narcotics.

In partnership with the DHS Domestic Nuclear Detection Office, CBP has also deployed nuclear and radiological detection equipment such as radiological detection portal monitors, radiation isotope identification devices, and personal radiation detectors Nationwide.

Using radiation portal monitors, CBP is able to scan 100 percent of mail and express consignment parcels, 100 percent of all trucks and personally-owned vehicles arriving from Canada and Mexico, and nearly 100 percent of all arriving maritime containerized cargo for the presence of radiological or nuclear materials.

In conjunction with CBP's many other initiatives, advancements in cargo, conveyance, and vehicle screening technology significantly increases CBP's ability to detect and interdict illegal drugs, radiological weapons and other dangerous materials, and continues to be a cornerstone of CBP's multi-layered border security strategy.

Thank you for the opportunity to testify today, and I am happy to answer any of your questions.

[The joint prepared statement of Mr. Owen, Mr. Luck, and Mr. Michelini follows:]

JOINT PREPARED STATEMENT OF TODD C. OWEN, EXECUTIVE ASSISTANT COMMISSIONER, OFFICE OF FIELD OPERATIONS, DEPARTMENT OF HOMELAND SECURITY; SCOTT A. LUCK, ACTING DEPUTY CHIEF, U.S. BORDER PATROL, DEPARTMENT OF HOMELAND SECURITY; AND, DENNIS J. MICHELINI, ACTING EXECUTIVE DIRECTOR, OPERATIONS, AIR AND MARINE OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION, DEPARTMENT OF HOMELAND SECURITY

JULY 25, 2017

Chairwoman McSally, Ranking Member Vela, and distinguished Members of the committee. It is a pleasure to appear before you today on behalf of U.S. Customs and Border Protection (CBP) to discuss how border security technology enables us to achieve our strategic and operational border security objectives, specifically in combating the flow of illegal aliens and dangerous contraband into the United States.

Along the more than 5,000 miles of border with Canada, 1,900 miles of border with Mexico, approximately 95,000 miles of shoreline, and at 328 ports of entry (POE) and more than 40 countries across the globe, CBP's U.S. Border Patrol (USBP), Air and Marine Operations (AMO), and Office of Field Operations (OFO) secure our borders and associated air space and maritime approaches to prevent illegal entry of people and materials, including dangerous drugs, into the United States. The border environment in which CBP works is dynamic and requires continual adaptation to respond to emerging threats and changing conditions. We appreciate the partnership and support we have received from this committee, whose commitment to the security of the American people has enabled the continued deployment of advanced technology assets needed to secure the border.

As President Trump has stated, "Homeland Security is in the business of saving lives, and that mandate will guide our actions." Through a series of Executive Orders (EOs), the President has taken steps to enhance border security, promote public safety, minimize the threat of terrorist attacks by foreign nationals, and protect

American workers from unfair foreign competition. The President's fiscal year 2018 budget proposes significant investments to support all of those goals while implementing the EOs.

In January, the President signed the Executive Order entitled *Border Security and Immigration Enforcement Improvements* (EO 13767). Included in the budget is a total of $2.6 billion in enhancements in high-priority border security technology, tactical infrastructure, assets, and equipment, including $975 million for border security technology, assets, and equipment.

Our testimony today discusses some of the advanced technology used by CBP front-line agents and officers to deter, detect, and interdict illegal cross-border activity, at and between POEs. Technology enhances CBP's operational capabilities by increasing our ability to detect and apprehend individuals illegally crossing the border, to detect dangerous goods and materials concealed in cargo and vehicles, and to detect and interdict illegal activity in the air and maritime domains. Advanced detection and surveillance technology is a critical element of CBP's multi-layered border security strategy to deploy the right mix of personnel, technology, and tactical infrastructure to enable us to meet the everyday challenges of a dynamic border threat environment. For CBP, the use of technology in the border environment is an invaluable force multiplier that increases situational awareness and allows us to detect illegal activity—including unauthorized border-crossers—and interdict dangerous drugs—and those who attempt to smuggle them—faster and safer.

TECHNOLOGY AT THE PORTS OF ENTRY

Smugglers use a wide variety of tactics and techniques for concealing drugs and other contraband through POEs. CBP officers regularly find drugs concealed in body cavities, taped to bodies (body carriers), hidden inside vehicle seat cushions, gas tanks, dash boards, tires, packaged food, household and hygiene products, checked luggage, and concealed in construction materials on commercial trucks. CBP incorporates advanced detection equipment and technology, including the use of Non-Intrusive Inspection (NII) equipment and radiation detection technologies to maintain robust cargo, commercial conveyance, and vehicle inspection regimes at our POEs.

NII technology is a critical element in CBP's ability to detect contraband as well as materials that could pose nuclear and radiological threats. These systems enable CBP officers to examine cargo conveyances such as shipping containers, commercial trucks, and rail cars, as well as privately-owned vehicles, for the presence of contraband without physically opening or unloading them. This allows CBP to work smarter and faster in detecting contraband, while expediting legitimate trade and travel. NII technologies deployed to our Nation's land, sea, and air POEs include large-scale X-ray and gamma-ray imaging systems, as well as a variety of portable and handheld technologies.

As of July 1, 2017, 301 Large-Scale (LS) NII systems are deployed to, and in between, our POEs. In fiscal year 2016, LS–NII systems were used to conduct more than 6.45 million examinations resulting in more than 2,600 seizures and over 359,000 pounds of seized narcotics. NII systems are particularly valuable in detecting concealed contraband in vehicles and cargo containers. With the help of NII, on July 22, 2017, CBP officers assigned to the San Ysidro POE seized 4.54 kilograms (10 pounds) of fentanyl, 11.31 kilograms (24.96 pounds) of methamphetamine, and 1.10 kilograms (2.43 pounds) of mannitol hidden in the quarter panels of a 2012 Toyota Corolla driven by a 26-year-old female U.S. citizen accompanied by a 27-year-old female U.S. citizen passenger. The budget proposes $109.2 million to build upon prior year investments and will be used to recapitalize the current small-scale (SS) and LS NII technology fleet. This funding will allow CBP to remain on track to ensure the NII fleet is operating within its service life by fiscal year 2024, and will help CBP continue to use NII to safely, quickly, and effectively detect a wide range of contraband imported using a variety of conveyances, thereby facilitating lawful trade and travel.

Personal vehicles are not the only means by which smugglers attempt to transport illegal drugs and other contraband across the border. For example, just a couple of weeks ago, CBP officers using NII equipment and canine teams at the Pharr International Bridge cargo facility discovered 2,746 pounds of marijuana and 50.70 pounds of cocaine, worth almost $1 million, over the course of just 3 days.[1]

Furthermore, as an integral part of the DHS comprehensive strategy to combat nuclear and radiological terrorism, CBP scans all arriving conveyances and containers with radiation detection equipment prior to release from the POE. In part-

[1] *https://www.cbp.gov/newsroom/local-media-release/cbp-field-operations-seizes-over-900k-marijuana-and-cocaine-commercial*.

nership with the DHS Domestic Nuclear Detection Office (DNDO), CBP has deployed nuclear and radiological detection equipment, including Radiation Portal Monitors (RPM), Radiation Isotope Identification Devices (RIID), and Personal Radiation Detectors (PRD) to 328 POEs Nation-wide.[2] Utilizing RPMs, CBP is able to scan 100 percent of all mail and express consignment mail and parcels; 100 percent of all truck cargo; 100 percent of personally-owned vehicles arriving from Canada and Mexico; and nearly 100 percent of all arriving sea-borne containerized cargo for the presence of radiological or nuclear materials. Since the inception of the RPM program in 2002 through June 2017, CBP has scanned approximately 1.4 billion conveyances for radiological contraband, resulting in more than 6.1 million alarms, all of which have been successfully resolved at the proper level.

In conjunction with CBP's many other initiatives, advancements in cargo and conveyance screening technology provide CBP with a significant capacity to detect dangerous materials and other contraband and continue to be a cornerstone of CBP's multi-layered security strategy.

TECHNOLOGY INVESTMENTS ALONG THE BORDER

Thanks to the support of Congress, CBP continues to deploy proven, effective technology to strengthen border security operations between the POEs—in the land, air, and maritime environments. With enhanced detection and surveillance capabilities, USBP and AMO can improve their situational awareness remotely, direct a response team to the best interdiction location, and warn the team of any additional danger otherwise unknown along the way. As a result, these investments increase CBP's visibility of illegal activity along the border, our operational capabilities, and the safety of front-line law enforcement personnel. The terrain along the border between the United States and Mexico is extremely diverse, consisting of desert landscape, mountainous terrain, and urban areas. Tailored to address an area's risk and environmental challenges, CBP deploys a combination of fixed and mobile technology assets, with short-, medium-, and long-range persistent surveillance capabilities to maintain situational awareness of the varying border environments.

Fixed, Persistent Surveillance

Integrated Fixed Tower (IFT) systems are one of technologies used by USBP that are being deployed to the Southwest Border in Arizona. IFTs provide long-range, persistent surveillance. An IFT system automatically detects with radars, identifies and classifies items of interest with day and night cameras, and tracks the items of interest at the Command and Control Center using a COP that integrates data, video, and geospatial locations of selected items of interest. The first IFT system became operational in the Nogales Area of Responsibility in August 2015. The second IFT system became operational in May in the Douglas Area of Responsibility. The third system has been installed and will undergo system acceptance testing this September in the Sonoita Area of Responsibility. The budget supports these critical assets by including $22.4 million in fiscal year for operations and maintenance of the IFT program and $17.4 million for IFT program procurement, construction, and improvements.

Remote Video Surveillance Systems (RVSS) are another fixed technology asset used by USBP in select areas along the Southwest and Northern Borders. These systems provide short-, medium-, and long-range, persistent surveillance from towers or other structures. The RVSS uses cameras, radio, and microwave transmitters to send video to a control room, enabling the control room operator to remotely detect, identify, classify, and track targets using the video feed. Existing RVSSes are being upgraded with newer cameras and additional towers. The budget includes $20.0 million in fiscal year to sustain RVSS. An additional $46.2 million is provided for procurement, construction, and improvements. This funding will be used to support the deployment of the RVSS capability to the Rio Grande Valley Sector.

In some areas along the Southwest Border, USBP also uses Unattended Ground Sensors (UGS), which provide short-range, persistent surveillance. These sensors support our capability to detect, and, to a limited extent, track and identify subjects. Sensor capabilities include seismic, passive infrared, acoustic, contact closure, and magnetic, although these capabilities are not necessarily available in all deployed UGS. When a ground sensor is activated, an alarm is communicated to an operations center. Some UGS are used in conjunction with Imaging Sensors (IS). The UGS/IS include an imaging capability to transmit images or video back to the oper-

[2] As of June 30, 2017, CBP currently has 1,276 RPMs, 3,316 RIIDs, and 34,387 PRDs operational systems deployed Nation-wide.

ations center. As with UGS, UGS/IS are monitored in a centralized system and geospatially tracked.

Fixed systems provide persistent surveillance coverage to efficiently detect unauthorized border crossing and incursions by suspected drug smugglers. Once detection is confirmed, USBP can quickly deploy the appropriate personnel and resources to interdict. Without fixed-system technology such as IFT, RVSS, and UGS, USBP's ability to detect, identify, classify, and track illicit activity would be significantly limited.

Mobile and Relocatable Capabilities

Working in conjunction with fixed surveillance assets, USBP also uses mobile and relocatable systems to address areas where rugged terrain and dense ground cover may allow adversaries to exploit blind spots or avoid the coverage of fixed systems. Mobile and relocatable technology assets provide USBP with the flexibility to adapt to changing border conditions and threats.

Along the Southwest Border, Mobile Surveillance Capability (MSC) systems provide long-range, mobile surveillance. They include radar and camera sensors mounted on USBP vehicles. An agent deploys with the vehicle to operate the system, which automatically detects and tracks items of interest and provides the agent/operator with data and video of the observed subject.

Mobile Vehicle Surveillance Systems (MVSS) are short-, and medium-range, mobile surveillance equipment. They consist camera sensors on telescoping masts mounted on USBP vehicles. A USBP agent deploys with the system, which detects, tracks, identifies, and classifies items of interest using the video feed. The agent/operator observes activity on the video monitor to detect intrusions and assist agents/officers in responding to those intrusions. The budget includes $3.2 million to provide operation and sustainment for MVSS, and an additional $1.6 million for procurement, construction, and improvements to fulfill operational needs on the Southern and Northern Borders.

Another system is the Agent Portable Surveillance System (APSS). Mounted on a tripod, it provides medium-range, mobile surveillance and can be transported by two or three USBP agents. Two agents remain on-site to operate the system, which automatically detects and tracks items of interest and provides the agent/operator with data and video of selected items of interest.

CBP's Tactical Aerostats and Re-locatable Towers program, originally part of the Department of Defense (DOD) re-use program, uses a mix of aerostats, towers, cameras, and radars to provide USBP with increased situational awareness over a wide area. This capability has proven to be a vital asset in increasing USBP's ability to detect, identify, classify, and track activity. Since initial deployment in 2012, these systems have been responsible for detecting more than 180,000 illegal border incursions of aliens and smugglers, leading to the seizure of approximately 180 tons of narcotics and related contraband. In this fiscal year alone, USBP agents, with the assistance of existing aerostats and re-locatable towers, have seized 62 tons of narcotics, and caught more than 20,000 illegal border crossers detected by aerostats. The budget includes $34.8 million in fiscal year for the Tactical Aerostats and Relocatable Towers Program to fund continued operations and maintenance costs.

Technology is critical to USBP border security operations. A tailored blend of complementary fixed, mobile, and portable surveillance systems increases USBP's effectiveness in targeting a high-risk areas, enabling rapid-response strategies to maximize limited manpower, and adjusting to seasonal and periodic traffic patterns.

TECHNOLOGY IN THE AIR AND MARITIME DOMAINS

AMO increases CBP's situational awareness, enhances its detection and interdiction capabilities, and extends our border security zones, offering greater capacity to stop threats before they reach our shores. Through the use of coordinated and integrated surveillance capabilities—including aviation, marine, tethered aerostats, and integrated, ground-based radars—AMO detects, interdicts, and prevents acts of terrorism and the unlawful movement of people, illegal drugs, and other contraband toward or across the borders of the United States. These assets provide multi-domain awareness for our partners across the Department, as well as critical aerial and maritime surveillance, interdiction, and operational assistance to our ground personnel.

AMO's maritime assets are tailored to the conditions of the environments in which we operate, and are equipped with the capabilities required to interdict attempted illicit smuggling of drugs and undocumented aliens. Often there is little time to interdict inbound suspect vessels, and AMO has honed its maritime border security response capability around rapid and effective interception, pursuit, and interdiction of these craft.

AMO employs high-speed Coastal Interceptor Vessels (CIV) that are specifically designed and engineered with the speed, maneuverability, integrity, and endurance to intercept and engage a variety of suspect non-compliant vessels in offshore waters, as well as the Great Lakes. Furthermore, AMO's Small Vessel Stand-off Detection radiation detection capability increases the probability of detecting radiological and nuclear materials that might be used to attack the country. The transportable equipment is effective against small private or commercial vessels and can indicate a potential threat in advance of a boarding.

The budget also seeks significant investments in our aircraft fleet. For example, the budget includes $55.5 million in fiscal year to purchase two KA–350ER multi-role enforcement aircraft (MEA). The MEA is the optimal sensor-equipped aircraft for surveillance operations in regions such as the Southern Border, Northern Border, and maritime environments where terrain, weather, and distance pose significant obstacles to border security operations. The MEA further serves as a force multiplier for law enforcement and emergency response personnel, facilitating the rapid-response deployment of equipment, canines, and people. The multiple roles of the MEA include presently maritime with planned ground and air surveillance as well as air-to-air tracking and LETC.

P–3 Long-Range Trackers and Airborne Early Warning Aircraft provide critical detection and interdiction capability in both the air and marine environment. Their sophisticated sensors and high-endurance capability greatly increase AMO's range to counter illicit trafficking. CBP P–3s are an integral part of the successful counter-narcotic missions operating in coordination with the Joint Interagency Task Force—South. The P–3s patrol a 42 million-square-mile area that includes more than 41 nations, the Pacific Ocean, Gulf of Mexico, Caribbean Sea, and seaboard approaches to the United States. In fiscal year 2016, CBP's P–3 operational efforts led to the total seizure or disruption of more than 193,000 pounds of cocaine with an estimated wholesale value of $2.5 billion.

Helicopters are also critical components of AMO's aircraft fleet. UH–60 Black Hawk helicopters are critical to border security operations, being the only helicopters in our fleet with medium-lift capability (i.e., the ability to carry eight agents with full gear). The UH–60 is rugged enough to support interdiction and life-saving operations in hostile environments, at high altitudes in the desert, over open water, and in extreme cold. The budget includes $14.1 million in fiscal year to purchase one UH–60 Medium-Lift Helicopter (MLH).

Another important asset is the DHC–8 Maritime Patrol Aircraft (MPA). It bridges the gap between strategic assets, such as the P–3 and Unmanned Aircraft System (UAS), and the smaller assets providing support in littoral waters.

AMO's aircraft have received a number of technological upgrades to increase their utility. Avionics upgrades to the AS–350 helicopter allow operators to focus more of their attention on the mission, making them more effective. AMO has also added electro-optical infrared detection technology to its fixed-wing, light observation aircraft, greatly increasing its tactical capabilities.

UASs are an increasingly important part of CBP's layered and integrated approach to border security. The UAS consists of an unmanned aircraft, sensors, communication packages, pilots, and ground control operators. UASs are used for surveillance, detection, and other mission requirements along the Southwest Border, Northern Border, and in the drug source and transit zones. The UAS program has achieved over 43,500 flight hours since it began in fiscal year and has been credited with interdicting or disrupting the movement of cocaine and marijuana with an estimated wholesale value of $170 million. CBP can equip four UAS aircraft with Vehicle and Dismount Exploitation Radar (VADER) sensor systems, which can detect human movement along the ground. Since 2012, VADER has detected over 51,600 people moving across the Southwest Border.

UAS and P–3 aircraft are equipped with technology that provides full-motion video capture for real-time and forensic analysis. This advanced detection and communication system enables AMO to disseminate live images and other sensor data to operational users, increasing response effectiveness and speed.

The budget proposes $2.5 million to expand the small Unmanned Aircraft Systems (sUAS) pilot projects and develop an official program of record. USBP needs this capability to surveil locations between the POEs in remote, isolated, and inaccessible portions of our borders. The sUAS needs to provide ground reconnaissance, surveillance, and tracking capabilities to support the USBP surveillance tasks of predicting, detecting, tracking, identifying, and classifying suspected items of interest. The ability to persistently and discreetly surveil remote areas along portions of the border is critical to USBP's ability to secure the border.

Perhaps the most important advancements come in the area of data integration and exploitation. New downlink technology allows AMO to provide a video feed and

situational awareness to its law enforcement partners in real-time. In addition, the Minotaur mission integration system will allow multiple aircraft to share information from multiple sources, providing a never-before-seen level of air, land, and maritime domain awareness. As the Minotaur system evolves, it will provide even greater awareness for a larger number of users.

AMO also combats airborne and maritime smuggling with an integrated long-range radar architecture comprised of ground-based radars and elevated radars deployed on tethered aerostats. AMO, in partnership with DOD, operates and maintains a network of more than 120 long-range radars providing a wide-area, persistent surveillance capability to detect and identify cooperative and non-cooperative aircraft traveling within or near the United States and crossing its borders. This network provides AMO the capability to detect and respond to air and maritime threats to the homeland, including organizations attempting to traffic contraband into the United States.

AMO's Tethered Aerostat Radar System (TARS) monitors the low-altitude approaches to the United States. With 8 aerostat sites—6 along the Southwest Border, one in the Florida Keys, and one in Puerto Rico—the TARS elevated sensor mitigates the effect of the curvature of the earth and terrain-masking limitations associated with ground-based radars, enabling maximum long-range radar detection capabilities. In fiscal year 2014 through fiscal year 2016, TARS was responsible for detecting 86 percent of all suspected air smuggling flights approaching the Southwest Border from Mexico. The budget provides support for the Tethered Aerostat Radar System program. The $41.2 million requested will provide for the annual system operations, system upkeep, maintenance and supply of Government personnel, and real property needs such as site and facility leases and expenses, for the full program. This funding will sustain the steady-state operations of the system while also retiring major threats from technical and program risks to system operations and health stemming from aging technology, diminishing manufacturing sources, and emerging regulatory requirements.

A vital component of DHS's domain awareness capabilities, AMO's Air and Marine Operations Center (AMOC) integrates surveillance capabilities and coordinates a response to threats to National security with other CBP operational components, including USBP, Federal, and international partners[3] to detect, identify, track, and support interdiction of suspect aviation and maritime activity in the approaches to U.S. borders, at the borders, and within the interior of the United States. Coordinating with extensive law enforcement and intelligence databases and communication networks, AMOC's command-and-control operational system, the Air and Marine Operations Surveillance System (AMOSS), provides a single display capable of processing up to 700 individual sensor feeds and tracking over 50,000 individual targets simultaneously. The eight TARS sites represent approximately 2 percent of the total integrated radars in AMOSS, yet were able to account for detecting 53 percent of all suspect target detections.

CBP is also pursuing improved border surveillance capabilities in the air domain. AMO is performing a formal Analysis of Alternatives (AOA) to review and assess multiple opportunities for extending a TARS-like surveillance capability beyond the next decade. A field test of promising key technologies is planned to take place in fiscal year 2018. In addition, AMO is participating in an interagency effort to assess the feasibility of moving its current air surveillance radar capabilities out of the L-Band spectrum so that the L-Band spectrum can be auctioned off for private sector use. If the move proves feasible, the proceeds of the auction would be used to transition to the new air surveillance capability.

As we continue to deploy border surveillance technology, particularly along the Southwest Border, these investments in fixed and mobile technology, as well as enhancements of domain awareness capabilities provided by the AMOC allow CBP the flexibility to shift more agents from detection duties to interdiction of illegal activities across our borders.

BORDER TECHNOLOGY REQUIREMENTS DEVELOPMENT

CBP is committed to effective and efficient resource allocation and works closely with other elements of DHS headquarters and fellow department components to ensure strategy-led, operationally-informed requirements development. This process enables DHS to effectively and efficiently execute acquisition strategies and budgets that address the broad range of complex border threats and challenges, including

[3] AMOC partners include the Federal Aviation Administration (FAA), the Department of Defense (including the North American Aerospace Defense Command (NORAD)), and the governments of Mexico, Canada, and the Bahamas.

illegal migration, smuggling of illegal drugs, human and arms trafficking, and the threat of terrorist exploitation of border vulnerabilities.

For example, CBP works closely with the DHS Science & Technology (S&T) Directorate to identify and develop technology to improve our surveillance and detection capabilities along our land and maritime borders. This includes investments in tunnel detection and tunnel activity monitoring technology; tactical communication upgrades, sUAS; low-flying aircraft detection and tracking systems, land and maritime data integration/data fusion capabilities, and border surveillance tools tailored to the Southwest and Northern Border, including unattended ground sensors/tripwires, upgrades for mobile surveillance systems, slash camera poles, and wide-area surveillance.

In addition to collaboration with our DHS partners, as part of CBP's efforts to seek innovative ways to acquire and use technology, CBP formed a partnership with DOD to identify and reuse excess DOD technology. To date, CBP has acquired several types of technology, including thermal imaging equipment, night vision equipment, and tactical aerostat systems, which increase CBP's situational awareness and operational flexibility in responding to border threats. We will continue to pursue additional opportunities to leverage DOD excess equipment. We will do this in a sustainable way by considering the full life-cycle costs of the DOD equipment we are considering before acquiring it.

CONCLUSION

Technology is a primary driver of all land, maritime, and air domain awareness. CBP's risk-based deployment of technology allows us to achieve our strategic and operational enforcement objectives at our POEs, along U.S. borders, and in the air and maritime approaches. The information obtained from NII, RPMs, fixed and mobile surveillance systems, ground sensors, imaging systems, and other advanced aerial and maritime technologies enhances domain awareness, informs situational awareness, and better enables CBP to monitor, detect, identify, and appropriately respond to unauthorized crossings and contraband smuggling.

Ms. MCSALLY. Thank you.

The Chair now recognizes Mr. Luck for 5 minutes to testify.

Can you make sure your microphone is on?

STATEMENT OF SCOTT A. LUCK, ACTING DEPUTY CHIEF, U.S. BORDER PATROL, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. LUCK. Chairwoman McSally, Ranking Member Vela, Mr. Correa, and Members of the subcommittee, thank you for the opportunity to testify today on behalf of the men and woman of the U.S. Border Patrol to discuss our use of technology to secure the border.

Our Border Patrol operations along the Southwest Border are continuously challenged by evolving tactics and transnational criminal organizations and individuals.

The Border Patrol uses sophisticated technology, a critical element in our layered border strategy to enhance our situational awareness and to detect changes in threat levels and criminal flows across the border.

Thanks to the support of this subcommittee, CBP continues to deploy capable technology resources to increase our ability to detect illegal activity along the Southwest Border and our ability to more efficiently, effectively, and safely respond, as appropriate, to potential threats.

With enhanced detection and surveillance capabilities, Border Patrol agents can improve their situational awareness remotely, direct our agents to the best interdiction location, and warn of any other additional danger otherwise unknown along the way.

As a result, these investments increase the Border Patrol's visibility on the border, our operational capabilities, and the safety of our front-line law enforcement personnel.

As many on this subcommittee know, the terrain along the border between the United States and Mexico is extremely diverse, consisting of deserts, mountains, and urban areas.

Tailored to address an area's risk and environmental challenges, CBP deploys a combination of fixed, mobile, and relocatable technology assets with short-, medium-, and long-range persistence surveillance capabilities to maintain situational awareness of the varying border environments.

For example, integrated fixed towers deployed along the border in Arizona provide a long-range persistence surveillance. These tower systems automatically detect and track items of interest and provide centralized operators with video and geospatial location of suspected items of interest for identification and appropriate action.

Remote video surveillance systems, RVSS, are another fixed technology asset used by the U.S. Border Patrol to provide persistent surveillance in select areas along the Southwest and Northern Borders.

These systems, which use cameras, radio, and microwave transmitters to send video to a control room, enable the Border Patrol to remotely detect, identify, classify, and track targets effectively.

Mobile technology mounted on vehicles or carried by agents, is used in conjunction with fixed assets and provides the Border Patrol flexibility and agility to adapt to the changing border conditions and threats.

Tactical aerostats and relocatable towers acquired as part of the Department of Defense reuse program, have also proven to be a vital asset in increasing CBP's situational awareness and our ability to detect, identify, and track illegal cross-border activity.

Mobile surveillance technology systems enable Border Patrol agents to position the technology where it is needed at a specific moment, extend our observational capabilities, and increase the accuracy and speed of our response.

In addition to the use of surveillance technology, collaboration and information sharing with our law enforcement partners is a key component of building situational awareness and response capabilities along our Southwest Border.

We work closely with our CBP partners, especially Air and Marine Operations, as well as multiple DHS, Federal, international, State, Tribal, and local law enforcement agencies.

Technology is critical to the Border Patrol's border security operations. A tailored blend of fixed, mobile, and portable surveillance systems that complement one another and work in conjunction with other elements of our operations, including intelligence, partnerships, and tactical infrastructure, increases the Border Patrol's effectiveness in addressing high-risk and seasonal or periodic traffic patterns and enables rapid response strategies to maximize limited manpower.

Chairwoman McSally, Ranking Member Vela, Mr. Correa, and distinguished Members of the subcommittee, thank you for the opportunity to appear before you today.

In closing, I would like to thank the men and women of the United States Border Patrol for their hard work and dedication to duty, who unselfishly protect our Nation 24 hours a day, 365 days a year. I look forward to answering your questions.

Ms. MCSALLY. Thank you, Mr. Luck.

I think I pronounced your name wrong—Mr. Michelini, not Michelini?

Mr. MICHELINI. Michelini. That is correct.

Ms. MCSALLY. OK, so it is Michelini? OK. The Chair now recognizes Mr. Michelini for 5 minutes.

STATEMENT OF DENNIS J. MICHELINI, ACTING EXECUTIVE DIRECTOR OF OPERATIONS, AIR AND MARINE OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MICHELINI. Good morning, Chairwoman McSally, Ranking Member Vela, and Mr. Correa and distinguished Members of the subcommittee. It is an honor to appear before you today to discuss the technology used by CBP Air and Marine Operations, AMO, in securing our Nation's borders.

A critical component of CBP's border security mission, AMO secures the United States from transnational threats, including terrorism, weapons and drug smuggling, and other illicit activities throughout our four core competencies: Interdiction, investigations, domain awareness, and contingencies in National taskings.

Throughout my 22 years in law enforcement, first as a Border Patrol agent and then as an air interdiction pilot, I have personally witnessed a significant increase in the development and deployment of technology to aid in the security of our borders, the result of which has, without doubt, improved our efficiency and effectiveness in fulfilling our law enforcement mission.

Throughout the use of coordinated and integrated surveillance capabilities, including aviation, marine-tethered aerostats and integrated ground-based sensors, AMO detects, interdicts, and prevents the unlawful movement of people, illegal drugs, and other contraband toward or across the borders of the United States.

Our technology assets provide multi-domain awareness for our partners across CBP and the Department of Homeland Security, as well as critical aerial and maritime surveillance interdiction and operational assistance to our ground personnel.

AMO's aerial surveillance capabilities are enhanced through recent investments and deployments of fixed-wing, rotary, and unmanned aircraft. These assets are equipped with a range of advanced sensor systems tailored to specific operational environments and provide critical detection interdiction capability.

Sophisticated sensors and high-endurance aerial capabilities greatly increase AMO's effectiveness in countering illicit cross-border activity.

AMO operates the Air and Marine Operations Center, AMOC, which is a state-of-the-art law enforcement domain awareness center. AMOC uses advanced surveillance systems and intelligence databases to detect threats to homeland and coordinate their interdiction.

AMO also combats airborne and maritime smuggling with an integrated long-range radar architecture comprised of ground-based radars and elevated radars deployed on tethered aerostats.

Across our entire program, AMO contributed to more than 4,300 arrests, 55,000 apprehensions, and the interdiction of nearly 200,000 pounds of cocaine in fiscal year 2016. AMO lends its capabilities to a variety of Federal partners, including the U.S. Coast Guard and the United States Navy, by conducting counter narcotic operations in the southeast coastal and source and transit zones.

We are the leading provider of airborne detection and monitoring to the Joint Interagency Task Force South. We also provide direct assistance to partner nations with the shared interest in border security, most notably Mexico and Canada.

Moving forward, we will continue to work with our CBP and other partners to enhance our detection, investigation, and interdiction capabilities, to address emerging threats and to protect America's security interests along the Nation's border in source and transit zones and our own customs waters and within the Nation's interior.

Chairwoman McSally, Ranking Member Vela, Mr. Correa, and distinguished Members of the subcommittee, thank you for this opportunity to testify today. I look forward to answering your questions.

Ms. MCSALLY. Thank you.

The Chair now recognizes Ms. Gambler for 5 minutes to testify.

STATEMENT OF REBECCA GAMBLER, DIRECTOR, HOMELAND SECURITY AND JUSTICE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Ms. GAMBLER. Good morning, Chairman McSally, Ranking Member Vela, Ranking Member Correa, Members of the subcommittee. I appreciate the opportunity to testify at today's hearing to discuss GAO's work on DHS efforts to acquire and deploy various technologies along U.S. borders.

DHS has employed a variety of assets in its efforts to secure the Southwest Border, including various land-based surveillance technologies. GAO has reported on DHS's management and oversight of these surveillance technologies under the former Secure Border Initiative and the Department's more recent plans.

My remarks today will summarize some of GAO's past reports, as well as some preliminary observations from our on-going work for this subcommittee on CBP's various surveillance technologies.

More specifically CBP has made progress in deploying technologies along the Southwest Border. This includes fixed and mobile surveillance systems, agent portable devices, and ground sensors. These technologies have aided CBP's border security efforts.

As of July 2017, CBP has completed deployment of selected technologies to areas in Arizona, Texas, and California. For example, CBP has reported deploying all planned Remote Video Surveillance Systems, or RVSS, and Mobile Surveillance Capabilities systems, or MSCs, to Arizona.

CBP has also reported deploying 15 of 53 planned Integrated Fixed Towers, or IFTs, to Arizona. CBP has deployed all planned MSC systems to Texas and California.

Although CBP has made this progress in technology deployments, we have also reported that CBP could do more to strengthen its management of technology programs and better assess the contributions of surveillance technologies to border security efforts.

For example, CBP has previously experienced delays in some of its technology programs. We have also previously reviewed CBP's schedules and life-cycle cost estimates for the IFT, RVSS, and MSC programs. We compared these schedules and estimates to best practices.

Overall the schedules and estimates for the programs reflected some but not all best practices. We found that CBP could take further action to better ensure the reliability of its schedules and cost estimates by more fully applying those best practices.

CBP has taken steps toward addressing our recommendations in these areas, such as providing us with updated schedules for some of the technology programs which have showed notable improvements in quality. We are continuing to review CBP's schedules and estimates as part of our on-going work for this subcommittee.

Further, CBP has identified the mission benefits of surveillance technologies, such as improved situational awareness and agent safety. CBP has also begun requiring Border Patrol to record data within its database on whether or not an asset, such as a camera, assisted in an apprehension or seizure.

These are positive steps toward helping CBP assess the contributions of its surveillance technologies to border security. However, CBP needs to develop and implement performance measures and analyze data it is now collecting to be able to fully assess the contributions of its technologies to border security.

In closing, we are continuing to examine CBP's use of technologies for border security as part of our on-going work. We will also continue to follow up on actions taken by CBP in response to our recommendations for improving management and measurement of the agency's land-based surveillance technologies.

This concludes my oral statement, and I am happy to answer any questions Members have.

[The prepared statement of Ms. Gambler follows:]

PREPARED STATEMENT OF REBECCA GAMBLER

JULY 25, 2017

Chairwoman McSally, Ranking Member Vela, and Members of the subcommittee: I am pleased to be here today to discuss the Department of Homeland Security's (DHS) efforts to acquire and deploy land-based surveillance technology and the extent that DHS measures the effectiveness of these deployed technologies to secure U.S. borders. The Southwest Border continues to be vulnerable to cross-border illegal activity, and DHS reported apprehending about 409,000 illegal entrants and making about 14,000 seizures of drugs along the Southwest Border in fiscal year 2016. Within DHS, U.S. Customs and Border Protection's (CBP) U.S. Border Patrol (Border Patrol) is the Federal agency with primary responsibility for securing the

National borders between U.S. ports of entry.[1] CBP has divided geographic responsibility for the Southwest Border among 9 Border Patrol sectors.[2]

DHS has deployed a variety of land-based surveillance technologies, which Border Patrol uses to assist its efforts to secure the border and to apprehend individuals attempting to cross the border illegally. In November 2005, DHS launched the Secure Border Initiative (SBI), which was responsible for developing a comprehensive border protection system using technology, known as the Secure Border Initiative Network (SBInet). Under the SBInet program CBP acquired 15 fixed-tower systems at a cost of nearly $1 billion, which are deployed along 53 miles of Arizona's 387-mile border with Mexico. In January 2011, in response to internal and external assessments that identified concerns regarding the performance, cost, and schedule for implementing the systems, the Secretary of Homeland Security announced the cancellation of further procurements of SBInet surveillance systems, though CBP continued operating the existing SBInet systems. That same month, CBP introduced the Arizona Border Surveillance Technology Plan (ATP). The ATP includes a mix of radars, sensors, and cameras to help provide security for the Arizona border. In June 2014, CBP developed a separate plan that incorporates the ATP, and includes the rest of the Southwest Border—the Southwest Border Technology Plan. Under the Southwest Border Technology Plan, CBP has plans to extend land-based surveillance technology deployments to the remainder of the Southwest Border, beginning with selected areas in Texas and California.

Over the years, we have reported on the progress DHS has made and challenges it faces in implementing its border security efforts. My statement discusses: (1) The status of CBP efforts to deploy land-based surveillance technology and (2) CBP's efforts to measure the effectiveness of these technologies.

This statement is based on reports and testimonies we issued from 2011 through 2017 that examined DHS efforts to secure the U.S. border.[3] It also includes selected updates on DHS's efforts to address our previous recommendations related to the ATP and our on-going work for this subcommittee on border surveillance technologies. Our reports and testimonies incorporated information we obtained and analyzed from officials from various DHS components. More detailed information about our scopes and methodologies, including which DHS components we interviewed for the work, can be found in our published reports and testimonies.

For the updates on our ATP work and our on-going work, we reviewed documents from DHS on actions it has taken to address findings and recommendations made in the prior reports on which this statement is based. For updates on the status of selected land-based surveillance technology programs, we reviewed CBP and DHS documents and examined cost and schedule data for each technology program. We also interviewed program managers responsible for the overall activities of these programs, including actions to design, acquire, deploy, and test the technology systems, and manage Government and contractor efforts. As part of our on-going work related to the deployment of land-based technology along the Southwest Border, we conducted site visits to Arizona in November 2016 and April 2017 and to south Texas in March 2017. During these site visits we observed border surveillance operations and interviewed CBP officials who operate and utilize these technologies.

All of our work was conducted in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

---

[1] Ports of entry are facilities that provide for the controlled entry into or departure from the United States. Specifically, a port of entry is any officially designated location (seaport, airport, or land border location) where DHS officers or employees are assigned to clear passengers and merchandise, collect duties, and enforce customs laws, and where DHS officers inspect persons entering or applying for admission into, or departing the United States pursuant to U.S. immigration law.

[2] Each of the 9 Southwest Border Patrol sectors (Big Bend, Del Rio, El Centro, El Paso, Laredo, Rio Grande Valley, San Diego, Tucson, and Yuma) has a headquarters with management personnel and these sectors are further divided geographically into varying numbers of stations, with agents assigned to patrol defined geographic areas.

[3] These include: *GAO, Arizona Border Surveillance Technology Plan: Additional Actions Needed to Strengthen Management and Assess Effectiveness*, GAO–14–368 (Washington, DC: Mar. 3, 2014), *Homeland Security Acquisitions: Major Program Assessments Reveal Actions Needed to Improve Accountability*, GAO–15–171SP (Washington, DC: Apr. 22, 2015), *Border Security: DHS Surveillance Technology, Unmanned Aerial Systems and Other Assets*, GAO–16–671T (Washington, DC: May 24, 2016), and *Homeland Security Acquisitions: Earlier Requirements Definition and Clear Documentation of Key Decisions Could Facilitate On-going Progress*, GAO–17–346SP (Washington, DC: Apr. 6, 2017). See Related GAO Products page for additional reports.

CBP HAS MADE PROGRESS DEPLOYING SURVEILLANCE TECHNOLOGY ALONG THE SOUTHWEST BORDER, BUT COULD TAKE ADDITIONAL ACTIONS TO STRENGTHEN MANAGEMENT OF ITS PROGRAMS

CBP Has Made Progress Toward Completing Milestones for Technology Deployment

Since 2014, we have reported multiple times on the progress CBP has made deploying technologies under the ATP. We reported in May 2016 that CBP had initiated or completed deployment of technology to Arizona for 6 programs under the ATP.[4] In addition to deploying technologies under the ATP, CBP's 2014 Southwest Border Technology Plan extended technology deployments to the remainder of the Southwest Border, beginning with selected areas in Texas and California. As of July 2017, CBP completed deployment of select technologies to sectors in Arizona, Texas, and California. For example, in our April 2017 assessment of DHS's major acquisitions programs, we reported that CBP completed deployments of 7 Integrated Fixed Tower (IFT) systems to the Nogales Border Patrol station within the Tucson sector in Arizona, and was working to deploy the remaining 46 towers to other sectors in Arizona.[5] As of July 2017, CBP reported deploying an additional 8 IFT systems, for a total of 15 of 53 planned towers. CBP has also made changes to the IFT program. Specifically, rather than expanding IFT capabilities to the Wellton Border Patrol station within the Yuma sector in Arizona as originally planned, CBP now plans to replace 15 existing SBInet fixed-tower systems with IFT systems.[6] CBP also reported that it had completed Remote Video Surveillance System (RVSS) and Mobile Surveillance Capability (MSC) deployments to Arizona as planned under the ATP, and deployed 32 MSC systems to Texas and California.[7] Additionally, CBP completed contract negotiations with the RVSS program for follow-on contract option periods to deploy RVSS to two stations in the Rio Grande Valley sector in Texas. The deployment status of the IFT, RVSS, and MSC technologies is shown below in table 1. We will plan to report on the deployment status of Southwest Border surveillance technology, among other topics, in a forthcoming report.

[4] The ATP's 7 acquisition programs include fixed and mobile surveillance systems, agent portable devices, and ground sensors. The Mobile Video Surveillance System (MVSS) units to be procured under the ATP were redirected to Texas due to changing operational priorities. Its three highest-cost programs, which represent 97 percent of the ATP's estimated cost, are the Integrated Fixed Tower (IFT), Remote Video Surveillance System (RVSS), and Mobile Surveillance Capability (MSC).

[5] An IFT system consists of towers, among other things, ground surveillance radars and surveillance cameras mounted on fixed (that is, stationary) towers.

[6] These 15 SBInet surveillance systems were deployed to the Tucson and Ajo stations within the Tucson sector in Arizona. Border Patrol began using SBInet systems at the Tucson station in February 2010 and at the Ajo station in August 2010.

[7] An RVSS consists of day and night cameras, laser designator, mounted on monopoles, lattice towers, and buildings and differs from the IFT in, among other things, that the RVSS is an expansion of a legacy system and does not include radars, while the IFT is a new system with radars. An MSC is a stand-alone, truck-mounted suite of radar and cameras mounted 25 feet high on a truck that provides a display within the cab of the truck.

TABLE 1.—DEPLOYMENT STATUS OF SELECT TECHNOLOGIES ALONG THE SOUTHWEST BORDER AS OF JULY 2017

Technology Program	Location	Under Contract	Deployment		
			Started	Completed	
Integrated Fixed Tower (IFT).	Arizona	X	X		Customs and Border Protection (CBP) completed deployments of IFT systems to the Nogales and Douglas Border Patrol stations in Arizona. Four additional Border Patrol stations are scheduled—Sonoita; Casa Grande; Ajo; and Tucson. In addition, in January 2015, Border Patrol requested that CBP replace the 15 existing Secure Border Initiative Network (SBInet, "Block 1") fixed-tower systems in the Tucson sector (Border Patrol began using these systems at the Tucson station in February 2010 and at the Ajo station in August 2010) with new IFT systems, rather than expanding IFT capabilities and deploying these systems to a new area of responsibility in Yuma, Arizona at the Wellton station, as originally planned.
Remote Video Surveillance System (RVSS).	Arizona	X		X	In December 2016, CBP completed deployments of all new and upgraded RVSS systems that it planned to deploy in Arizona.
	Texas-Rio Grande City and McAllen stations within the Rio Grande Valley sector.	X (under the Arizona contract)			CBP officials stated they completed a site laydown study for RVSS sites, and according to CBP, the program has been working with Johns Hopkins University Applied Physics Laboratory to examine video field of view. CBP signed off on-site laydowns in April 2016. CBP also stated that the current contract includes an option to expand RVSS into the Rio Grande Valley sector and that current program funding allows for RVSS to be deployed in the McAllen and Rio Grande City Border Patrol stations.

	Texas and other areas.	.....	.....	.....	CBP plans to deploy RVSS to the remaining planned sites within and outside of Texas. CBP officials stated that this would be a new procurement action; therefore, CBP plans to release a new Request for Proposal and has initiated the development of the acquisition strategy for these remaining areas of responsibility within and outside of Texas.
Mobile Surveillance Capability (MSC).	Arizona, Texas and California.	X	.....	X	CBP reported that as of December 2016 it had completed deployments of all MSC systems to Arizona, Texas (Big Bend, Del Rio, and El Paso sectors), and California, (San Diego and El Centro sectors).

[1]Source: GAO analysis of CBP data. GAO–17–765T.

CBP Has Made Progress in Implementing GAO's Prior Recommendations, but Could Take Additional Actions to Strengthen Management of Its Programs

In March 2014, we assessed CBP's efforts to develop and implement the ATP.[8] Specifically, we recommended that CBP, among other things: (1) Apply scheduling best practices; (2) develop an integrated schedule; and (3) verify life-cycle cost estimates. DHS concurred with some of our recommendations and has taken actions to address some of them, which we discuss below.

Program Schedules.—In March 2014, we found that CBP had a schedule for deployment for each of the ATP's 7 programs, and that 4 of the programs would not meet their originally-planned completion dates. Specifically, we found that the 3 highest-cost programs (IFT, RVSS, and MSC), had experienced delays relative to their baseline schedules, as of March 2013.[9] We also reported that CBP had at least partially met the four characteristics of reliable schedules for the IFT and RVSS schedules and partially or minimally met the four characteristics for the MSC schedule. Scheduling best practices are summarized into four characteristics of reliable schedules—comprehensive, well-constructed, credible, and controlled (i.e., schedules are periodically updated and progress is monitored).[10] We assessed CBP's schedules as of March 2013 for the three highest-cost programs and reported in March 2014 that schedules for two of the programs at least partially met each characteristic (i.e., satisfied about half of the criterion), and the schedule for the other program at least minimally met each characteristic (i.e., satisfied a small portion of the criterion).[11] For example, the schedule for the IFT program partially met the characteristic of being credible in that CBP had performed a schedule risk analysis for the program, but the risk analysis did not include the risks most likely to delay the program or how much contingency reserve was needed. For the MSC program, the schedule minimally met the characteristic of being controlled in that it did not have valid baseline dates for activities or milestones by which CBP could track progress. We recommended that CBP ensure that scheduling best practices are applied to the IFT, RVSS, and MSC program schedules. DHS concurred with the recommendation and stated that CBP planned to ensure that scheduling best practices would be applied, as outlined in our schedule assessment guide, when updating the three programs' schedules.

In response to our March 2014 recommendation regarding applying scheduling best practices, CBP provided us with updated program schedules for the IFT, RVSS, and MSC programs. Based on our assessment of updated program schedules for the IFT, RVSS, and MSC that CBP had completed as of January 2017, CBP has made significant improvements in the quality of the programs' schedules, but the programs' schedules had not met all characteristics of a reliable schedule. For example, CBP has improved the quality of its products for analyzing and quantifying risk to the programs' schedules; however, CBP could improve the documentation of these analyses and the prioritization of the programs' risks. While CBP has taken positive steps we continue to believe that by ensuring that all scheduling best practices are applied, CBP could help ensure the reliability of its programs' schedules and better position itself to identify and address any potential delays in its programs' commitment dates.

Integrated Master Schedule.—In March 2014, we also found that CBP had not developed an Integrated Master Schedule for the ATP in accordance with best practices. Rather, CBP had used separate schedules for each program to manage implementation of the ATP, as CBP officials stated that the ATP contained individual ac-

---

[8] GAO–14–368.

[9] The baseline schedule is to represent the original configuration of the program plan and to signify the consensus of all stakeholders regarding the required sequence of events, resource assignments, and acceptable dates for key deliverables. The current schedule is to represent the actual plan to date.

[10] GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules*, GAO–16–89G (Washington, DC: Dec. 2015). We developed this guide through a compilation of best practices that Federal agencies and industry use. According to this guide, for a schedule to be comprehensive, among other things, the schedule should: (1) Capture all activities, as defined in the work breakdown structure; (2) reflect what resources are needed to do the work; and (3) establish the duration of all activities and have specific start and end dates. To be well constructed, among other things, a schedule should have all of its activities sequenced in the order that they are to be implemented with the most straightforward logic possible. To be credible, the schedule should reflect the order of events necessary to achieve aggregated products or outcomes, and activities in varying levels of the schedule map to one another. Moreover, a schedule risk analysis should be conducted to predict a level of confidence in meeting the program's completion date. For a schedule to be controlled, the schedule should be updated periodically using actual progress and logic to realistically forecast dates for program activities, and a baseline schedule should be maintained to measure, monitor, and report the program's progress.

[11] GAO–14–368.

quisition programs rather than integrated programs. However, collectively these programs are intended to provide CBP with a combination of surveillance capabilities to be used along the Arizona border with Mexico, and resources are shared among the programs.[12] We recommended in March 2014 that CBP develop an Integrated Master Schedule for the ATP. CBP did not concur with this recommendation and maintained that an Integrated Master Schedule for the ATP in one file undermines the DHS-approved implementation strategy for the individual programs making up the ATP, and that the implementation of this recommendation would essentially create a large, aggregated program, and effectively create an aggregated "system of systems." DHS further stated at the time that a key element of its plan has been the disaggregation of technology procurements. As we reported in March 2014, this recommendation was not intended to imply that DHS needed to re-aggregate the ATP's 7 programs into a "system of systems" or change its procurement strategy in any form. The intent of the recommendation was for DHS to insert the individual schedules for each of the ATP's programs into a single electronic Integrated Master Schedule file in order to identify any resource allocation issues among the programs' schedules. We continue to believe that developing and maintaining an Integrated Master Schedule for planned technologies could allow CBP insight into current or programmed allocation of resources for all programs as opposed to attempting to resolve any resource constraints for each program individually.

Life-cycle Cost Estimates.—In March 2014, we also reported that the life-cycle cost estimates for the technology programs under the ATP reflected some, but not all, best practices. Cost-estimating best practices are summarized into four characteristics—well-documented, comprehensive, accurate, and credible. Our analysis of CBP's estimate for the ATP and estimates completed at the time of our March 2014 review for the two highest-cost programs—the IFT and RVSS programs—showed that these estimates at least partially met three of these characteristics: Well-documented, comprehensive, and accurate. In terms of being credible, these estimates had not been verified with independent cost estimates in accordance with best practices.[13] We concluded that verifying life-cycle cost estimates with independent estimates in accordance with cost-estimating best practices could help better ensure the reliability of the cost estimates, and we recommended that CBP verify the life-cycle cost estimates for the IFT and RVSS programs with independent cost estimates and reconcile any differences. DHS concurred with this recommendation, but stated then that it did not believe that there would be a benefit in expending funds to obtain independent cost estimates and that if the costs realized to date continued to hold, there may be no requirement or value added in conducting full program updates with independent cost estimates.[14]

We recognize the need to balance the cost and time to verify the life-cycle cost estimates with the benefits to be gained from verification with independent cost estimates. As part of our updates on CBP's efforts to implement our 2014 recommendations, CBP officials told us that in fiscal year 2016, DHS's Cost Analysis Division would begin piloting DHS's independent cost estimate capability on the RVSS program. According to CBP officials, this pilot is an opportunity to assist DHS in developing its independent cost estimate capability. CBP selected the RVSS program for the pilot because the program was at a point in its planning and execution process where it can benefit most from having an independent cost estimate performed, as these technologies are being deployed along the Southwest Border beyond Arizona. According to CBP officials, DHS's Cost and Analysis Division (CAD) completed its independent cost estimate for the RVSS program in August 2016, and that in February 2017 CBP had completed its efforts to verify the RVSS program cost estimate with CAD's independent cost estimate, which is part of the CAD pilot. However, as of July 2017, CBP has not yet provided us with the final reconciliation of the independent cost estimate and the RVSS program cost estimate, as we recommended in 2014. CBP officials have not detailed similar plans for the IFT. We

---

[12] According to scheduling best practices, an Integrated Master Schedule is a critical management tool for complex systems that involve a number of different projects, such as the ATP, to allow managers to monitor all work activities, how long activities will take, and how the activities are related to one another. We concluded in March 2014 that developing and maintaining an Integrated Master Schedule for the ATP could help provide CBP a comprehensive view of the ATP and help CBP better understand how schedule changes in each individual program could affect implementation of the overall plan.

[13] GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO–09–3SP (Washington, DC: Mar. 2, 2009).

[14] An independent cost estimate provides an independent view of expected program costs that tests the program office's estimate for reasonableness. Independent cost estimates frequently use different methods and are less burdened with organizational bias, helping to provide decision makers with insight into a program's potential costs.

continue to believe that independently verifying the life-cycle cost estimates for the IFT and RVSS programs and reconciling any differences, consistent with best practices, could help CBP better ensure the reliability of the estimates.

CBP HAS MADE PROGRESS ASSESSING PERFORMANCE OF SURVEILLANCE TECHNOLOGIES, BUT HAS NOT FULLY APPLIED PERFORMANCE METRICS OR ASSESSED THE CONTRIBUTIONS OF ITS TECHNOLOGIES

We reported in March 2014 that CBP had identified mission benefits of its surveillance technologies to be deployed along the Southwest Border, such as improved situational awareness and agent safety. However, the agency had not developed key attributes for performance metrics for all surveillance technologies to be deployed, as we recommended in November 2011.[15] Further, we also reported in March 2014 that CBP did not capture complete data on the contributions of these technologies, which in combination with other relevant performance metrics or indicators, could be used to better determine the impact of CBP's surveillance technologies on CBP's border security efforts and inform resource allocation decisions. We found that CBP had a field within its Enforcement Integrated Database for data on whether technological assets, such as SBInet surveillance systems, and non-technological assets, such as canine teams, assisted or contributed to the apprehension of illegal entrants and seizure of drugs and other contraband; however, according to CBP officials, Border Patrol agents were not required to record these data. This limited CBP's ability to collect, track, and analyze available data on asset assists to help monitor the contribution of surveillance technologies, including its SBInet system, to Border Patrol apprehensions and seizures and inform resource allocation decisions. We recommended that CBP require data on asset assists to be recorded and tracked within its database, and once these data were required to be recorded and tracked, that it analyze available data on apprehensions and technological assists—in combination with other relevant performance metrics or indicators, as appropriate—to determine the contribution of surveillance technologies to CBP's border security efforts. CBP concurred with our recommendations and has implemented one of them. Specifically, in June 2014, CBP issued guidance informing Border Patrol agents that the asset assist data field within its database was now a mandatory data field. Therefore, agents are required to enter any assisting surveillance technology or other equipment.

Further, as part of our updates on CBP's efforts to implement our 2014 recommendations we found that in May 2015, CBP had identified a set of potential key attributes for performance metrics for all technologies to be deployed under the ATP. However, CBP officials stated at that time that this set of performance metrics was under review as the agency continued to refine the key attributes for metrics to assess the contributions and impacts of surveillance technology on its border security mission.[16] In our April 2016 update on the progress made by agencies to address our findings on duplication and cost savings across the Federal Government, we reported that CBP had modified its time frame for developing baselines for each performance measure and that additional time would be needed to implement and apply key attributes for metrics.[17] According to CBP officials, CBP expected these performance measure baselines to be developed by the end of calendar year 2015, at which time the agency planned to begin using the data to evaluate the individual and collective contributions of specific technology assets deployed under the ATP. Moreover, CBP planned to use the baseline data to establish a tool that explains the qualitative and quantitative impacts of technology and tactical infrastructure on situational awareness in specific areas of the border environment by the end of fiscal year 2016. Although CBP had initially reported it had expected to complete its development of baselines for each performance measure by the end of calendar year 2015, as of March 2016, it was adjusting the actual completion date, pending test and evaluation results for recently deployed technologies to the Southwest Border.

In our April 2017 update on the progress made by agencies to address our findings on duplication and cost savings across the Federal Government, we reported that CBP had provided us a case study that assessed technology assist data, along with other measures such as field-based assessments of capability gaps, to deter-

[15] GAO–14–368 and *Arizona Border Surveillance Technology: More Information on Plans and Costs Is Needed before Proceeding*, GAO–12–22 (Washington, DC: Nov. 4, 2011).

[16] GAO–15–404SP.

[17] GAO, *2016 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO–16–375SP (Washington, DC: Apr. 13, 2016).

mine the contributions of surveillance technologies to its mission.[18] This is a helpful step in developing and applying performance metrics. However, the case study was limited to one border location and the analysis was limited to select technologies. To fully implement our recommendation, CBP should complete its efforts to fully develop and apply key attributes for performance metrics for all technologies deployed and begin using the data to evaluate the individual and collective contributions of specific technologies, fully assess its progress in implementing planned technologies, and determine when mission benefits have been fully realized. Until CBP completes this effort it will not be well-positioned to fully assess its progress in implementing the ATP and determining when mission benefits have been fully realized.

Chairwoman McSally, Ranking Member Vela, and Members of the subcommittee, this concludes my prepared statement. I will be happy to answer any questions you may have.

Ms. MCSALLY. Thank you, Ms. Gambler.

I now recognize myself for 5 minutes for questions.

Chief Luck and Director Michelini, air assets are a critical part of the technology integrated to build situational awareness for both operational level but also tactical level.

Air has been critical in the Tucson sector, but we have lost a bit of our air capability in that sector, and we understand that we are going to lose some more in the future here.

I understand there is increased activity in other sectors but still 50 percent of the marijuana comes from through Tucson sector. Especially in the hot summer we have a number of deaths in the desert and the air assets are very critical to getting to people before it is life-threatening.

So could you share what the impact has been of decrease in air in the Tucson sector and any plans you have to further decrease it? Because this is a concern of ours. We have made some great gains and we feel that we are potentially going to shift away from that should we lose some more air.

Mr. LUCK. As far as flight hours, is that what your concern is?

Ms. MCSALLY. Flight hours and assets, yes.

Mr. MICHELINI. OK. So we execute about 95,000 flight hours a year. That has been a pretty consistent number with us. There has been more movement. I mean, as—Tucson has gained a more of a control of the border than it was 10 years ago when the flight hours were much higher than they are right now.

But in the process of actually Tucson and them getting a hold of—and more maintenance of their border, we have seen a shift in flows to south Texas. So there has been a movement of flight hours and funding toward the south Texas area.

I don't necessarily foresee Arizona to drop any further than it is right now. I don't believe that this drop in any way shows a lack of interest from Air and Marine into that area.

Tucson, as it is, is the largest branch we have.

Ms. MCSALLY. Yes.

Mr. MICHELINI. I would probably say the agents are somewhere around 80 total. It has more air assets than anybody else, and it also flies more than anybody else. So it is still, it is a center cog for us in that western side of the United States.

It has a large diversity of platforms. Well, first of all, the UAS flies out of there at our office. It has more flight hours than any

[18] GAO, *2017 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO–17–491SP (Washington, DC: Apr. 26, 2017).

other. We have Blackhawks that fly. We have Citations for air interdictions, and we have AS–350's and small fixed-wing aircraft. So it is a hub for us in the southwest region.

Ms. MCSALLY. Chief Luck, do you have any comments on that?

Mr. LUCK. I would just add, based on your opening statements, that we are testing other things, other unmanned aerial systems to fill a gap. We are going to test some with the small UAS in Arizona here coming next month. So that is a gap-filler, too, for needed air requirements in southern Arizona.

In south Texas and we are also testing them in Swanton, Vermont to see what the capability is. So we have come quite a long ways with regard to SUAS in filling gaps in air requirements.

Ms. MCSALLY. Great, thanks. Continuing on the air discussion, the VADER technology has been helpful, but the feedback that we get when I go down and visit is oftentimes there are several limitations, obviously to the unmanned aerial systems as to when they can fly and when that information is available.

We have talked several times since I have been the subcommittee chair about pushing forward to also have that capability on manned aircraft. I know you are piloting that, pardon the pun, but can you give an update on the process of getting the VADER technology on manned aircraft to provide more flexibility?

Mr. MICHELINI. Well, first let me say that we are hoping to expand the UAS capabilities with VADER in Sierra Vista. We are very close to moving it to a 24 by 5 operation. When you probably visited throughout this year, it was a 16 by 5.

So, you know, what happens with weather for that is we do exactly that you mentioned before. You get affected by weather for both take-offs and landings.

If we move to a 5 by 24 model, we can launch and recover around those weather patterns. We have done a few experiments with that on 24 by 5, and we get massive bumps in flight-hour availability. So that is our initial plan going forward.

As far as putting the VADER on a manned asset, yes, that is a bit out. Those are a few years out for having that available.

Ms. MCSALLY. So that is not being piloted right now?

Mr. MICHELINI. It is being piloted, but there is nothing physical right now I could tell you about.

Ms. MCSALLY. OK. So the time line for even knowing whether that is a possibility you are saying is several years?

Mr. MICHELINI. I don't believe it could be 7 years, but can I——

Ms. MCSALLY. Several, sorry, several not 7.

Mr. MICHELINI. Oh. No, can I get you a better time line on that?

Ms. MCSALLY. Absolutely. No, this is something we have been, you know, interested in for a while so it would be helpful to understand the plan for that and the timing for testing and evaluation and all that, so.

We are going to have a second round here. I am running out of my time. So I will now recognize Mr. Correa for 5 minutes.

Mr. CORREA. Thank you, Madam Chair.

Ms. Gambler, a couple questions. What were the lessons from the failed SBInet? Has CBP fixed the management costs and schedule problems that led to the failure of SBInet? Could we see more of the same with on-going and future CBP technology acquisitions?

Ms. GAMBLER. Sure. I will answer the middle question first if that is OK in terms of the——

Mr. CORREA. Take it away.

Ms. GAMBLER [continuing]. The cost and schedule. We have seen improvements, particularly in CBP's schedules for some of the different land-based surveillance technologies. So that has been a positive step that CBP has made toward addressing our recommendations.

In terms of the life-cycle cost estimate, specifically for the RVSS program, CBP and DHS have worked to conduct an independent life-cycle cost estimate and tried to reconcile that to the cost estimate that CBP has for the RVSS.

We will be working with CBP to get documentation of that and take a look at it. So we have seen progress being made on both schedules and the estimates and that progress is really positive.

In terms of your broader question, Ranking Member, about lessons learned and steps going forward, I think there are two key themes or lessons learned from our work looking at CBP's technology programs.

The first is that it is important for CBP to make sure the technology programs go through the DHS acquisition management process fully and completely. DHS's acquisition management process is a robust, valid, knowledge-based process, but CBP hasn't always insured that technology programs have moved through that process consistently. So they need to apply the acquisition management process consistently to their technology programs.

Second, and as I mentioned in my oral statement, it is important for CBP to put in place the metrics that we have been recommending for several years now so that they can really assess what we are getting out of our investments and technologies.

So those are the two things that we see as lessons learned and are important things for CBP to focus on going forward.

Mr. CORREA. Thank you. Ms. Gambler, a recent GAO report concluded that CBP lacked the metrics necessary to show whether or how the existing border wall contributes to border security.

Does it make sense to move forward with President Trump's multi-billion-dollar wall before CBP can show what kind of return the American taxpayers would get on their investment, if any? Is it possible, less costly, to have less intrusive border security measures that would be more effective?

Ms. GAMBLER. Ranking Member, that question gets at two key findings from GAO's work on infrastructure and technology along the border.

The first is we do think it is important for CBP to put metrics in place, both for tactical infrastructure to include the fencing that has been deployed, as well as technologies that I have mentioned.

The other important theme from our work is, and we have reported on this previously as it relates to technology, is the need for CBP to be able to document the investments it is making and why it is choosing to put certain technologies or certain assets in certain places.

So seeing that documentation about the types and locations and quantities of things that are being deployed is an important part of planning for these types of acquisitions.

Mr. CORREA. Just as a follow-up comment, 20 years ago in Los Angeles, a seizure of $2 billion of cash and drugs occurred, semi-truck stop, regular coming in and off dropping, you know, tons of drugs. Those were not going, you know, through the terrain. They were going through the border, border check points.

Yesterday, San Antonio, Texas about 20 undocumented individuals in a semi. So my point is you have got a wall yet you have got most of the traffic, according to most of the folks I have talked to at the border, through the check points, existing border check points.

So, you know, those are my questions. Do you invest in a border or do you invest in better X-ray machines at the border crossing stations? Comment or statement, thank you.

Ms. GAMBLER. I think that is absolutely the right questions that we should be asking. It is important for CBP to be able to provide information on their plans so that decision makers in Congress can evaluate those plans and determine what would be the most effective use of resources.

So I think you are asking a very important question about technology and infrastructure deployments.

Mr. CORREA. Thank you.

Madam Chair, I yield.

Ms. MCSALLY. The gentleman yields back.

The Chair now recognizes Mr. Smith from Texas.

Mr. SMITH. All right. Thank you, Madam Chair. Thank you all for your expertise and your dedication to our country. It really is a privilege for us to hear you all today. You are on the front lines. You know first-hand what is going on.

Mr. Luck, before I address some questions to you, let me preface the questions by saying that when I was first elected I represented over 100 miles of Texas-Mexico border. That sort of riveted my attention on the particular subject.

Over the years, I have seen some examples of what works and does not work. We all know we need a combination of physical structure, personnel, and technology. In San Diego, for example, you have a double fence that has succeeded in stopping illegal immigration by about 95 percent.

Years ago, I know you were in the El Paso sector, chief of operations there, but a former Member of Congress, Silvestre Reyes, was once the border sector chief there. He stationed Border Patrol agents very, very close together.

I don't know if it was 100 yards or whatever, and it was personnel intensive. But he stopped illegal immigration almost entirely. So that was an example of how that worked.

I know in Texas a number of years ago we tried, at great cost, a virtual fence, and basically had to abandon it, in part because of vandalism by the illegal immigrants, in part because of false positives by the sensors, and in part because we didn't have enough Border Patrol agents backing up the technology.

So I know technology has improved since then, and I guess I am saying that there are parts of the border that lend themselves more to one than another perhaps.

I wanted to ask you where you thought it would be most beneficial to have a physical structure along the border, where you

thought it might be most beneficial to have technology along the border?

Mr. LUCK. Thank you for the question, sir. It depends on the terrain and it depends on the threat. So in the urban areas, you want to have something that slows down the volume of the traffic flow. So we want to have a persistent impedance or impedance and denial system, such as a physical barrier.

But that in itself doesn't work on its own. So it is a part of a package that we are concentrating on as part of our new strategy as it relates to the Executive Order and it relates to operational control.

The first part of that is, of course, the impedance and denial, the deterrence and so forth. Then we have the domain awareness. That is knowing what we are going to do and what assets. That is the technology piece.

The access and mobility and having direct access to the border and roads and infrastructure is a third piece. The last piece, of course, is the agents.

So it is a combination of all four of those master capabilities that gets us to the operational control that we are looking for. That depends on the location and the threat.

Mr. SMITH. Right.

Mr. LUCK. So in California, as you mentioned, the physical barrier helps stop the flow, helps displace the traffic so that we can use technology assets, situational awareness, to detect that traffic and bring it to a law——

Mr. SMITH. Right.

Mr. LUCK [continuing]. Enforcement resolution.

Mr. SMITH. Would it be accurate to summarize what you just said as saying that in the urban areas and high-traffic areas a physical structure is necessary and in other areas maybe it would be more technology then physical structure?

Mr. LUCK. That is accurate, sir.

Mr. SMITH. OK.

Mr. LUCK. That is exactly what it is.

Mr. SMITH. Last week the President said something along the lines of 700 to 900 miles of physical structure along the border, roughly half the border—it is a 2,000-mile border on the south—on the southern part of the United States—but we have some fencing in place, obviously, some single, some double, some concrete. But would that 700 to 900 miles sound about right for where we need a physical structure?

Mr. LUCK. To be honest, sir, we haven't gotten that far.

Mr. SMITH. OK.

Mr. LUCK. We haven't gotten that far in determining what the years to follow will give us——

Mr. SMITH. Right.

Mr. LUCK [continuing]. Based on the budget. What we do have is a plan for 2017, a plan for 2018, and then a plan for 2019 to 2023. So——

Mr. SMITH. OK. Let's take the outside plan, 2019 to 2023. How many miles of physical structure are anticipated by then?

Mr. LUCK. We don't have that number yet.

Mr. SMITH. Oh, you don't. OK.

Mr. LUCK. That is something that we are still developing.

Mr. SMITH. OK.

Mr. LUCK. There is a lot of variables that go into that. As we put impedance and denial on the border and other systems to back that up, it may have a trend of different things and that will happen as a result. The adversary does have, has a vote in this.

Mr. SMITH. Right.

Mr. LUCK. So we don't want to put specifically from point A to point B if the need isn't there.

Mr. SMITH. Understand. If you look at the urban areas and if you look at the high-traffic areas, you are going to come up with several hundred miles. I don't know exactly what it would be either. But clearly there is a role for the fencing, sometimes a double fencing which has worked particularly well on the Southern Border, I think.

Mr. LUCK. Absolutely, sir.

Mr. SMITH. OK.

Mr. LUCK. That as well as in some areas, a patrol area that is in between, right?

Mr. SMITH. Right, correct. Thank you, Mr. Luck.

Thank you, Madam Chair.

Ms. MCSALLY. Thank you. The gentleman yields back.

The Chair now recognizes Ms. Barragán.

Ms. BARRAGÁN. Thank you.

Mr. Michelini, I represent the Port of Los Angeles and drones are becoming more prevalent in commercial and personal use, sometimes coming into the land and air space of ports and other security-sensitive entry points.

How is CBP dealing with security issues these drones present at ports? Is CBP working with the TSA and local law enforcement to address this problem?

Mr. MICHELINI. CBP is working with the FAA on drones. Those small drones are still mostly a FAA concern. Those aircraft aren't supposed to fly, I mean, above 500 feet so they can sort themselves out from a manned aircraft.

Specifically, around ports of entry, I am not up to speed on what any kind of CBP actions have done in that regard.

Ms. BARRAGÁN. OK. Does anybody else on the panel want to add anything to that or kind of address if there are any jurisdictional issues that need to be resolved?

Mr. MICHELINI. No, I am not aware of any jurisdictional issues. But I am aware that in the ports and in the critical infrastructure, we do work very closely with the local law enforcement to respond to any information that maybe, you know, indicate that there is drone activity in the area. But I am not aware of any jurisdictional issues.

Ms. BARRAGÁN. OK.

Mr. Luck, what cyber vulnerabilities has CBP identified in the Arizona Border Surveillance Technology Plan and what is CBP's cybersecurity strategy for the Southwest Border Technology Plan?

Mr. LUCK. Could you repeat that, please?

Ms. BARRAGÁN. Sure. What cyber vulnerabilities has CBP identified in the Arizona Border Surveillance Technology Plan, the ATP?

What is CBP's cybersecurity strategy for the Southwest Border Technology Plan?

Mr. LUCK. I would have to back to you on that. I don't have an answer for that question.

Ms. BARRAGÁN. OK. If you could——

Mr. LUCK. Absolutely.

Ms. BARRAGÁN [continuing]. Follow up, that would be great.

Mr. LUCK. Right.

Ms. BARRAGÁN. OK.

Mr. Luck, does CBP have the documented plan or strategy to achieve situational awareness along our borders?

Mr. LUCK. Yes, ma'am, and we get that through our requirements management process. Part of that is our C–GAP, Capability Gap Assessment Process, that we use to bring in what the gaps are in coverage and what gaps are that needed to be filled along the border.

Then from there—and that is a bottom-up approach. From there, we decide on what the best courses of action are whether that is surveillance, technology, or whether that is a system or physical barrier.

Ms. BARRAGÁN. OK.

Ms. Gambler, in March 2014 the GAO reported that the CBP schedules and life-cycle cost estimates for the Arizona Border Surveillance Technology Plan and its three highest cost programs, which represented 97 percent of the plan's total estimated cost, met some but not all best practices.

GAO recommended that CBP ensure that its schedules and cost estimates more fully address best practices such as validating cost estimates with independent estimates, and DHS concurred. What more remains to be done?

Ms. GAMBLER. Yes, Congresswoman. On the schedules themselves, CBP has provided us with updated schedules, and they have shown significant improvements in quality. So we are continuing to look at those schedules to determine the extent to which the revised schedules fully meet the intent of our recommendation.

As it relates to the life-cycle cost estimates, I want to talk about the estimates for two different programs: The RVSS and the IFTs. For the RVSS, DHS, and CBP—DHS has conducted an independent life-cycle cost estimate for the RVSS and has been working with CBP to reconcile those two estimates.

We will be obtaining follow-up documentation from CBP and DHS on that effort and can certainly follow up with you after we have had a chance to look at that and make our own analysis.

For the IFTs, we have not seen that CBP has yet done an independent life-cycle cost estimate for that program and in line with what we recommended, we think it is important that they do so.

Ms. BARRAGÁN. Do you have an estimate of a time line on when this might be done and we have something back?

Ms. GAMBLER. With regard to us looking at the independent life-cycle cost estimate and the reconciliation with the RVSS, we are actually following up with CBP on that. So hopefully we can get back to you on that pretty quickly.

Ms. BARRAGÁN. Great. Thank you.

I yield back.

Ms. MCSALLY. The Chair now recognizes Mr. Hurd from Texas for 5 minutes.

Mr. HURD. Thank you, Chairwoman, for your focus on this important issue, and I would like to echo my colleagues in thanking the panelists for being here.

With 820 miles of the border, I recognize the difficulty of you all's task, having spent 9½ years as an undercover officer chasing terrorists, nuclear weapon proliferators, you name it, I recognize how difficult it is to secure our border.

I was just proud of that, my first bill signed into law was actually something that helped Border Patrol agents make sure their pay wasn't getting cut. So this is something that is very important to me.

It is 2017, and I think we as a Government should have done a better job of helping you all deploy technology along the border to do your jobs.

I guess my first question is—and maybe this goes to you first, Mr. Luck and Mr. Owen, if you have opinions I would welcome that as well. Currently right now how is computer vision being used in border security?

Mr. LUCK. Computer vision?

Mr. HURD. Yes, sir.

Mr. LUCK. Could you help me address that?

Mr. HURD. Sure. You know, we have these fixed towers. We have sensor technology. We have all this data that is coming in. Are we using automated tools in order to determine whether the movement of something is dangerous or is something that requires interdiction by Border Patrol?

Mr. LUCK. Yes. I mean, we are doing some predictive stuff as you may know that we are using our partners. We have agents assigned to extend our borders, and we are reusing systems with our partners in different countries to help to predict what the traffic flows will be.

So those are all—and collecting information and using that information to help us better prepare for what is coming to the border. So we are using that. The systems that we use for processing has evolved.

To comment on Ms. Gambler's comments on how we track the assets that we do use, that has been implemented into our E3 system. So we are using an array, there is a lot of data coming in.

The intelligence agents that are out there have an apparatus in either their sectors or at the headquarters through operation through our Office of Intelligence to be able to collate the data——

Mr. HURD. Sure.

Mr. LUCK [continuing]. That they get and the intelligence.

Mr. HURD. Gotcha. Gotcha. So how much of the current system automates detection, right? In this day and age, we can deploy any number of systems, lidar, radar, fiber optic cable to detect a bunny rabbit from a human. We should be able to automate that event to where a computer can tell us that isn't a bunny rabbit or a deer or a cow.

I hope we can say if it was cow with fever tick or not with fever tick, but that is a whole other question in south Texas. Is that being done?

Mr. LUCK. As far as the systems we have with integrated fixed towers, in some of our mobile surveillance capabilities, that is being done where we have multiple layers, you have the radars, and then you have the cameras that skew to the movement.

Then an alarm that will go off in the control room that will, say, instead of 100 cameras that an officer, an agent has to look at, there is an alarm that goes off that says there has been an incursion——

Mr. HURD. Gotcha.

Mr. LUCK [continuing]. And then it skews over and it helps with that. So that is the automation that we are looking for. We have some work to do to connect everything so that it all talks together and with all the systems that we have amongst the components, but that is what we are striving for.

Mr. HURD. Right. So do you have an integrated picture back at headquarters or does the Joint Task Force West have an integrated picture down in San Antonio on the Southwestern Border?

Mr. LUCK. They don't have an integrated picture that they can cue to to look at the activity——

Mr. HURD. Gotcha.

Mr. LUCK [continuing]. And see that.

Mr. HURD. Does the individual agent on the ground—like, I was recently in Del Rio humping through some Carrizo cane and it is not a pleasant experience, especially at 105-degree weather.

If there was a detection event, does that individual agent that may be patrolling that part of the sector, do they get notification themselves?

Mr. LUCK. Yes, through our ICAD system.

Mr. HURD. Is that a walkie-talkie? What is the ICAD system?

Mr. LUCK. Right. The ICAD system is the system that they use in dispatch. When an underground sensor goes off, it will automatically hit and they will call it out and the agent can respond to it. That is what they use.

Mr. HURD. Madam Chair, if we could have another round?

Ms. MCSALLY. We are.

Mr. HURD. OK, great. I yield back the time I do not have.

Ms. MCSALLY. Thanks. The gentleman yields back.

We are starting a second round. I want to actually continue on with that line of questioning. Situational awareness to the actual agent is something that I have been pushing on since I have been the Chairwoman of the subcommittee.

If we are bringing information together, but it is back in the operations center or the personnel that are on the ground doesn't have that—you don't want to overload them with information, but decision-quality information for them is key. Getting that over a voice is not ideal, you know, given the technology that we have.

Similarly, the mobile surveillance cameras, last time I was out there, we were talking about how just the person at the truck has that situational awareness. So what sort of initiatives are on-going related to bringing the data and information together in a fused way?

But then also providing appropriate information to the agents so their SA is increased as they are out there putting their lives on the line?

Mr. LUCK. One of the things that we are working with now in the platform that we are using is tracking sign cutting and modeling system.

What that does is when an event takes place, automatically when the agent calls in, "Hey, I have got a sign of three that I am working," automatically that starts a track, either geospatial track or geolocator track of where that agent is and what he is doing.

So, what it does is it fills in the gaps and then other technology can be used to assist him in that arena. So they are doing it a lot and it tracks what the movements are, what technology is utilized and things that can be used.

Now, what we want to do—and that then transfers over when the agent makes an arrest. That transfers over to the E3 processing system so that it can be used to capture all of the event that took place.

Ms. MCSALLY. But the agent is still predominantly getting information by voice is the point, right?

Mr. LUCK. Right.

Ms. MCSALLY. I mean, is there any sort of requirement or something in the works for Blue Force Tracking? Again, some sort of iPad-like wristwatch-like situational awareness for the agent? We had a friendly fire death in our sector?

You know, that just builds their situational awareness so they can see where are the good guys, where are the bad guys, what is going on? So it is not just the guys in the air-conditioned ops center that are seeing that.

Mr. LUCK. Right. What we know that that is a gap, and we are trying to do that. Some of that is gaps in communication, in having access to systems that track that like a down screen. We are using it in some areas for SAUS, for example, that the agent has the ability to see where the SAUS sees.

But as far as the ability to have something on them that can be used to track it, there are comms issues with that, and there is an expense. Blue Force Tracking, of course, has to be negotiated with the union to try to get that as part of the picture.

Ms. MCSALLY. So what you are saying is there is no requirement or, you know, technology, development in its process or funded to specifically provide increased situational awareness to the agent on the ground?

Like, yes, I know you are talking about some ideas, but we don't actually have a program or a system or a requirement that is moving any of that forward that right now?

Mr. LUCK. Not that I know of, ma'am, to be honest with you.

Ms. MCSALLY. OK. Following up on the tactical UAVs, you talked about it. Can you give me a little update, your testing in Arizona upcoming? Where are you doing that?

Mr. LUCK. OK. So what we have done with the UAV is we worked with partnership with Air and Marine.

Ms. MCSALLY. Yes.

Mr. LUCK. We have got an MOU in place with the Federal Aviation Administration so we can test those. We have bought a suite of different capabilities, one being the quadcopter that can be up in the air for about 30 minutes or so.

The other is a Raven type where it can be longer distance for longer time. Then the other one has got a 3-hour timespan. We bought some of those and now we want to test those in an operational testing environment in Arizona, in south Texas, and in Swanton, Vermont coming up in September.

Ms. MCSALLY. OK. So will you follow up as to where you are doing that in Arizona? I might want to go out and scout?

Mr. LUCK. Absolutely, ma'am.

Ms. MCSALLY. Also, to go back on Ms. Barragán's line of questioning, are you considering a cybersecurity elements of that? If you are just—off the shelves can be great for quickly getting capabilities to the agents, but if they can be easily jammed or intercepted——

Mr. LUCK. Yes, ma'am.

Ms. MCSALLY [continuing]. Or taken over.

Mr. LUCK. That is part of it and we are reaching out to the industry and some of the things going on in Silicon Valley to help with the sensors and so forth.

Ms. MCSALLY. Great. I want to reiterate—brought it up several time. In southern Arizona right now near the border we do have Cochise College with a very robust UAV training capability. They have been wanting to partner with you all on this tactical UAV issue.

We have made some introductions. I think not everybody in the bureaucracy is talking to the right people, but we would love to follow up with that, especially during your testing and evaluation——

Mr. LUCK. Very good.

Ms. MCSALLY [continuing]. So that you are not reinventing the wheel if there are training capabilities out there already.

Mr. LUCK. Very good.

Ms. MCSALLY. I yield back for this round.

Mr. Correa, you are up for another 5 minutes.

Mr. CORREA. Thank you, Madam Chair. Just wanted to get back to Ms. Gambler. I didn't quite understand your answer when I asked if CBP had the matrix necessary to assess the effectiveness of and the existing border wall and possibly a proposed border wall. Do we have the matrix?

Ms. GAMBLER. CBP does not currently have metrics in place to assess the contributions that existing fencing is making to border security efforts. That is what we reported on in our report on existing fencing earlier this year.

We recommended that CBP put in place those metrics to include using the existing data they have to be able to assess what contributions fencing is having to border security.

Mr. CORREA. Thank you. Question to the panel, if I may? My prior life as the chair of Select Committee in California in the Senate of California and Mexico, I took a number of tours of the border area, San Ysidro, San Diego.

I noticed the California Highway Patrol has a station there where I believe every semi-truck that comes through is checked for safety every quarter to make sure every truck that comes by is up to California vehicle code.

No. 2, every semi, I believe, is checked for radiation, and they are also checked for other, you know, possible issues. My question to

you is, given that situation, that investment the State of California has made in assuring the safety of Californians, do you have that same relationship with the other border States in terms of coordinating, making sure you share information from California and New Mexico, Arizona, and Texas?

Mr. OWEN. Well, sir, I will tell at all the ports of entry along the Southwest Border it is very common to find the State authorities just outside our compound looking at the trucks for the road worthiness, the safety issues, as you mentioned there.

As for the radiation screening, that is a function that we perform within the ports of entry. Every truck, every passenger vehicle coming into the United States is first screened for radiation before it ever can leave the ports. We have been doing that since about 2002. Again, most people aren't aware of that activity that takes place.

We do coordinate with the State transportation police outside those gates on different activities and things of that nature. So that is a, what you see in California is very common along the larger land border crossings along the Mexican border.

Mr. CORREA. So I guess my question is—so I assume you do communicate with local, State, and authorities in terms of coordinating your data to make sure if there are any patterns there, you actually can pick them up?

Mr. LUCK. In terms of——

Mr. CORREA. Patterns of possible illicit activity?

Mr. LUCK. Oh, patterns. We do. Again we are members of the various task forces that work along the Southwest Border where that information is shared in terms of the tactics, what we are finding, the trends and things of that nature.

So I would argue that on the field operations side and I am sure on the Border Patrol side, communication with the State and local authorities along the border region is very strong.

Mr. CORREA. Secretary Kelly has mentioned that, right now, coordination, cooperation with Mexican authorities is actually very good. Again, my prior life, I took a tour of the southern Mexican border.

I noticed most of the vehicles coming into Mexico from south of Mexico were X-rayed. A lot of that data is then digitalized, sent to Mexico City, and I believe it was shared with Langley. So it added a whole layer of multi-layered defense.

Is that relationship still there? Does it exist? Has that expanded? Tell me, how are we working with our partners, not only south of the border, but around the world in terms of enhanced security.

As Secretary Kelly has said, you know, if those things, items get to the border, you have already kind of lost. You have got to interdict those illicit items before they actually get to the border.

Mr. LUCK. Right. Well, I will tell you that within the Office of Field Operations we have very strong partnerships at 52 seaports around the globe as part of our container security initiative where we identify high-risk shipments before they are headed this way. We have partnerships in Colombia, in Honduras, in Panama that are very effective in terms of the narcotics interdiction.

The activities at the port of entry, I think in the last 3 years since I have been in this position, very much improved relationship

with the Mexican authorities, to the point that in several locations in Arizona, we have Mexican customs that are in the United States conducting joint inspections with us as part of a unified cargo inspection process.

Reduces some redundancies. It helps facilitate the lawful trade and travel. Been very effective within Arizona. So I can speak for the field operations, the relationship with Mexico is very strong. I defer to the chief on——

Mr. CORREA. I am running out time. So very quickly, I would say it would be good to create a matrix to assess how effective that relationship is in stopping and inspecting and being effective at the border. Thank you very much.

I yield, Madam Chair.

Ms. MCSALLY. The gentleman yields.

The Chair now recognizes Mr. Hurd from Texas for 5 minutes.

Mr. HURD. Thank you. Thank you, Chairwoman. Again Mr. Luck, Mr. Owen, same question for both of you all, you know, take a minute, minute and a half. Mr. Luck, describe your dream tech scenario for the CBP of tomorrow.

Mr. LUCK. My tech scenario would be having the right mixture of—based on the threat, having the right mixture of technology and we can't do it alone—no piece of technology has ever made an apprehension, that informs and talks to all the other component pieces that we have within CBP.

So that that information is shared immediately to all components and agents and officers who need it. That would be my dream scenario.

We have systems out there that are stand-alone systems that we would need—that, in my view, we need to have speak to one another and share that information with whatever piece of technology that is, so that we are not redundant in those efforts and that we know exactly we have the same situational awareness regardless of who that operating entity is.

Mr. HURD. Good copy. Mr. Luck, please correct me if I am wrong, I feel like the existing technology that is being used—there is an overwhelming, there is too much of an operating burden on the person using it. We need technology that is a little bit more user-friendly.

We need to make sure that this is integrated, as you say, across the various elements, not just within a team within its particular sector, but across sectors and even back at headquarters.

As Chairwoman McSally was saying, getting that information in the hands of the individual agent, whether they are in their vehicle, on foot, humping through Carizzo cane and that allows them to do only what they can do, the hardest part of the interdiction.

In anything that I described, am I out of line?

Mr. LUCK. No, sir. That is appropriate.

Mr. HURD. Good copy. We are trying to get you some dinero to do all this, by the way. That is why I get frustrated with all this talk about a wall, because $24.5 million a mile, that is a lot of money.

You can deploy a lot of off-the-shelf technology to do what I just described for half a million dollars a mile. If we add this out to the

additional 1,350 miles of the border that doesn't have fencing, that is $33 billion.

I can use $32 billion of that for a lot of other things, like give you all's folks more pay for the hard work that they do. Give Mr. Michelini some more air assets to do what he does. That is where we are trying to go with this idea of a smart wall that leverages technology to make sure the men and women in Border Patrol are doing their thing.

Mr. Owen, same question to you.

Mr. OWEN. Yes, sir. Well, the technology that really is the cornerstone of our interdiction activities in the ports of entry, is the large-scale, nonintrusive inspection technology. What we need is technology that has the capability to keep that cargo flowing.

On the passenger side, we have drive-through, low-energy systems where the passengers, the travelers, can stay in the car as we scan the car safely for the presence of any contraband. Those have been a game-changer for us in the passenger arena.

What we have on the horizon, and what we are working with our science and technology director, as well as some of the vendors and manufacturers, is a similar drive-through systems for cargo.

The challenge we have with cargo trucks now is you generally have a single energy system. You have to take the driver out of the cab. You can't use a high-energy system on the driver. That slows things down.

So with those current systems, only about seven trucks an hour can be scanned. The technology that is on the horizon that I really see as a game-changer for our cargo inspections, is a multi-energy system that you can ratchet down to a low-energy version to scan the cab.

As the driver and the cab clears, you ratchet up the energy level to high-energy to penetrate the cargo. That will allow the trucks to continue to keep moving, not have to come to a stop. We estimate 10 times as many inspections can be done an hour with that technology.

Mr. HURD. That is great.

Mr. OWEN. So that is on the horizon. We are looking at several locations where we will be deploying that, and I really see that as a game-changer for us in terms of our interdiction efforts in cargo shipments.

Mr. HURD. Chairwoman, I think we should put that on the list.

Yes. My final question, and maybe it is for you Mr. Luck, or Ms. Gambler, how much money do we spend, you know, in a year, here, to this date, on tunnel detection?

Mr. LUCK. I don't know how much money we spend. I know that we are working a lot with partners on most recent tunnel detection capability. It is a vulnerability and a threat that we need to really think seriously about.

We are working with industry. We are certainly working with our partners from Israel to give us the latest and greatest. We have an apparatus to kind of get that best technology.

Mr. HURD. We are worried about tunnel detection under physical barriers like the existing fencing we have, is that correct?

Mr. LUCK. Yes, we are. Part of the plan for future fencing would be to put fiber optics in there to help with it.

Mr. HURD. OK.

Ms. Gambler.

Ms. GAMBLER. I would just add, I think we may have some data on that, and I would be happy to follow up with your office and provide what we have.

Mr. HURD. We will, as well. Thank you all very much.

Thank you for the indulgence, Madam Chairwoman.

Ms. MCSALLY. Absolutely.

The Chair now recognizes Mr. Rutherford for 5 minutes.

Mr. RUTHERFORD. Thank you, Madam Chair.

I am particularly drawn to the circle here, the apprehension life cycle, as you all call it, because I have often said the same thing about this wall concept, that, you know, a wall is not a barrier. It is just an impediment.

What we need is to provide you with the technology that you can detect, track, apprehend in a secure way, these folks who are coming over the border.

Let me ask. The technology when we visited the Southern Border specifically, it seemed like—as far as Fort Huachuca, they had pretty good integration of communications and intelligence going on.

Further east of that, the Rio Grande Valley, there didn't seem to have been as much in the way of technology being applied. It almost looked like they ran out of money or something, you know? Or maybe it is just in the next phase.

But it just didn't seem like the Rio Grande Valley was getting the attention that the other areas that we had observed had.

Mr. Luck, can you speak to that? The needs, specifically in the Rio Grande Valley.

Mr. LUCK. Yes, sir. You are right. We didn't have enough attention on Rio Grande Valley because the traffic was coming through Arizona. So our technology lay down and these things take time. Some of these options take more time than others. We are trying to get Arizona under control.

So and now the focus is on the Rio Grande Valley. So we are trying to bring technology in there and we will be bringing technology in there.

In the way of remote video surveillance systems and our ability to do persistent surveillance, we do have the DOD reuse tactical aerostats there that have been very, very good.

We have the help from our partners in Air and Marine with some of the systems and sensors that they have, as far as flight hours. Now we are trying to concentrate and move into some of our persistent surveillance technologies and relocatable towers.

That is what we want, to move into RGV. We can do it quicker and they have the sophisticated camera systems that will give those agents more situational awareness. In that area, as you know, the Carizzo cane problem, we have to have height to be able to see into that.

So we are also testing different technologies that will maybe help us get more of a situational awareness in that Carizzo cane, such as foliage-penetrating radars, and things of that nature to try to test new things that helps us get that better picture. But that is,

we are recognizing that we need to have more technology in the Rio Grande Valley.

Mr. RUTHERFORD. I believe there is a significant increase in the technology budget to help with that, correct?

Mr. LUCK. Yes, and we thank this committee for that.

Mr. RUTHERFORD. Let me ask because another piece of the life cycle, as you call it, the apprehension phase of that, takes boots on the ground.

Mr. LUCK. Absolutely.

Mr. RUTHERFORD. I mean you just have to have boots on the ground. It is just that simple.

Mr. LUCK. Yes, sir.

Mr. RUTHERFORD. Is there anything that we can do to help you all in that process, acquiring more boots for the ground, the training, the recruitment, all of that?

Mr. LUCK. We are working very, very diligently with that. HRM has made a lot of advances, over 40 improvements in their pre-employment process. We are doing some things with waivers with dedicated people that have proven their integrity, with waivers of the polygraph. So and there is a robust——

Mr. RUTHERFORD. Is that helping?

Mr. LUCK. Yes, sir.

Mr. RUTHERFORD. OK.

Mr. LUCK. There is a robust effort toward recruitment right now.

Mr. RUTHERFORD. Very good.

Madam Chair, I yield back.

Ms. MCSALLY. Thank you. The gentleman yields back.

I am gonna do one more round, if you don't mind?

Mr. CORREA. Sure.

Ms. MCSALLY. Great. Thank you.

Ms. Gambler, you talked about—on several hearings, we have talked about the starting to measure the use of technology in apprehensions in order to better understand the metrics of whether the technology is helping.

Do we have any assessments? I mean, we have been talking about this for over a year, since I have been the subcommittee chair. Do we have any assessments of how any of the technologies are assisting in the apprehensions, or do we not yet have enough time of doing that?

Ms. GAMBLER. So in response to the recommendation that we made in our report on surveillance technologies from a few years ago, Chairwoman, CBP has provided us with one sample of how they have tried to look at metrics. So we have been evaluating that, but we need to see them do it more systematically for across the border.

So in order to adjust our recommendation we really need to see that CBP and Border Patrol are both looking at this from a more systematic perspective.

Ms. MCSALLY. All right. Thanks.

I am wondering, Mr. Luck, the deployment of IFTs and some of the other technology more recently in Arizona, is there any sort of assessments on that you could—short-term assessments on the effectiveness of that?

Obviously, you don't want correlation to equal causality because you don't know whether you are deterring activity or whether things are shifting for different reasons. But do you have any sort of feedback on how the IFTS and other technology are working in Arizona?

Mr. LUCK. So the reports that I am getting from the short time that they have been on live with the last towers in IFT in Douglas, the view sheds and the area that they can cover and the workability of those systems are functioning properly. It is a great asset and a needed asset in those environments.

MSCs, all the RVSS, the refresh that we are doing periodically for the RVSS until we can get the replacement is really working well in Arizona, and other places as well.

Ms. MCSALLY. Great. So at this point that is anecdotal, obviously, but, I mean, it is good feedback from those that are out there in charge building their situational awareness. It is going to be helpful to figure out the metrics or the measurement, right, and the integration with the other systems.

Is that fair, Ms. Gambler?

Ms. GAMBLER. That is right. We are happy to, you know, help provide feedback to CBP on that process as well as they are developing metrics. That is something that we have talked about and offered in the past.

Ms. MCSALLY. Great. Thank you.

Oh, go ahead. Yes?

Mr. LUCK. Ma'am, if I could just add on to the status on one of the recommendations from the GAO as far as our system E3, our processing system and the ability for agents to use a check-down box as a response to adding technology to the apprehension and the processing phase?

Ms. MCSALLY. Yes.

Mr. LUCK. That has been accomplished and is working well. So they have a drop-down box that has to be checked regarding what technology and other assets, and they can make multiple choices as——

Ms. MCSALLY. Right.

Mr. LUCK [continuing]. As it relates to the apprehension.

Ms. MCSALLY. That is great. Mr. Owen, you talked about technology that is maybe on the cutting edge here, the multi-energy system, and the NII technology being helpful. But the reality is we still have massive amounts of opioids, synthetic opioids, the hard drugs that are, you know, killing Americans right now in a crisis level, coming mostly through the ports of entry.

So what other technologies do we need in order to get what we are missing? I mean, we know what we are getting, but we are obviously missing a lot still because of the epidemic that we have going on in our country. So what else——

Mr. OWEN. Yes.

Ms. MCSALLY [continuing]. What else do we need?

Mr. OWEN. Yes, and it is very challenging. I mean, clearly they hide in the numbers: 76 million passenger vehicles that crossed the Southwest Border last year and another 6 million trucks.

It is very difficult to inspect all of those so we rely on intelligence. We rely on our advanced targeting capabilities, the advanced information that we have.

Then oftentimes it comes down to the instinct and training of the officers on primary where they just sense something is wrong and they send those individuals.

The current Fentanyl challenge is compounded by the two main pathways. We have the Fentanyl from China that is primarily entering through the international mail system, as well as the express courier hubs. The volume is just overwhelming in that environment.

E-commerce continues to skyrocket. I think there were about 360 million parcels last year, and it significantly increased this year. So very, very difficult in that environment and as well as on the Southwest Border. They hide in the numbers.

I think we have very dedicated men and women that use all of the tools that this committee and others have provided us. I think we are effective, but there is stuff that gets through, no doubt.

Ms. MCSALLY. What is your sense—actually I think it is important for people to realize that they are coming in from China through e-commerce.

Mr. OWEN. Yes.

Ms. MCSALLY. What is your sense of the percentage that is coming through that versus coming up through the border?

Mr. OWEN. I am not sure I have a percentage. I can tell you though that the testing that we have done and the purity of the Chinese Fentanyl coming through the mail and through the express is very close to 100 percent. It is very, very strong, very, very deadly.

The purity of the Fentanyl coming across the Southwest Border is much less. It is still a very significant threat, but you have got two different challenges that you are dealing with. Hopefully with our engagement with our international partners, we will see some relief in that area as well.

Ms. MCSALLY. OK. Thanks for highlighting that. Time is up.

The Chair now recognizes Mr. Correa.

Mr. CORREA. Thank you, Madam Chair.

Very quickly again to Mrs. Gambler, what remains to be done in order for the agency to better measure the effectiveness of its capabilities? Is CBP using all of the tools available in the best way possible, both for border security and measuring performance?

I say that from the following perspective that we talk about a lot of things we can do at the borders. Smart border, inland ports, new technology that, in my opening remarks I talked about some of the agents not being able to talk to each other.

They could see each other, but their communication devices weren't effective, and that reminds me of the Grenada invasion, you know, a couple of decades ago. We still have that same situation.

Meat and potatoes, basically investing in common everyday technology to make our personnel much more effective. Multi-energy system that you are talking about, Mr. Owen, I took a tour of a San Diego, I am not gonna mention the names, of a manufacturer

in San Diego that apparently had deployed some of these systems in the Middle East, not here, but in the Middle East.

Yet they were able to detect organics of drugs. You could actually could drive the trucks through, and I believe it was 10 to 20 seconds they could fully check a truck. If they saw anything negative then you would pull them over to secondary inspection.

So again, a lot of tools in the toolbox, a lot of technology, yet the meat-and-potatoes stuff still needs to be addressed. And that is where I think these metrics of measuring what is most cost-effective from the perspective of the taxpayers and public safety is important.

Like the Chairperson was saying right now, now you are talking about direct shipments from China, you know, directly through the mail. There is another challenge, and I wouldn't know how do you even begin to address that one.

But again, these are all the challenges that we have to look at, and where do we begin to invest? I think we have got to come back to the metrics.

Open statement, anybody care to address it?

Ms. GAMBLER. Ranking Member, I would add, from our perspective and what our work has shown, I mean, I think there are two, you know, kind-of, you know, key steps that are part of this process. As one that we need to see the department and CBP just set the metrics.

We have been recommending metrics in the border security area for several years. So they actually need to make decisions on what they want to measure and set what those metrics are.

The second step in that is that CBP collects a lot of data as an agency, and certainly what Chief Luck was describing in terms of them now requiring asset assist information, for example, to be entered into their database. That is a really positive step.

But what they need to do now is use the data they have systematically to measure relative to the metrics and goals that they have set.

So those are really two, you know, key fundamental steps that we think are an important part of this and assessing what we are getting out of the investments.

Mr. CORREA. Any other comments from the others?

Thank you. Madam Chair, I yield.

Ms. MCSALLY. OK. Well, I appreciate it. The gentleman yields back.

We were just talking up here. I think there is some of the themes here are worth as we are looking toward a border security bill to consider working together on some of the integrating technology, and increasing situational awareness in the port of entry technology. Those are some of our do-outs that we are gonna follow up on as we look to a future legislation.

I want to thank the witnesses for your valuable testimony. I thought it was a good discussion, and Members for their questions. Members of the committee may have some additional questions for the witnesses. I think you also have some that you took for the record as well. I would ask you to respond to these in writing. Pursuant to committee rule VII(D) the hearing will be open for 10 days.

Without objection, the committee now stands adjourned.
[Whereupon, at 11:26 a.m., the subcommittee was adjourned.]

○