ASSESSING THE DEPARTMENT OF HOMELAND SECURITY'S EFFORTS TO COUNTER UNMANNED AIRCRAFT SYSTEMS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT, MANAGEMENT, AND ACCOUNTABILITY

AND THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

MARCH 31, 2022

Serial No. 117–49

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

47–767 PDF WASHINGTON : 2022

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

SUBCOMMITTEE ON OVERSIGHT, MANAGEMENT, AND ACCOUNTABILITY

J. LUIS CORREA, California, *Chairman*

DINA TITUS, Nevada
DONALD M. PAYNE, JR., New Jersey
RITCHIE TORRES, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*
PETER MEIJER, Michigan, *Ranking Member*
DAN BISHOP, North Carolina
DIANA HARSHBARGER, Tennessee
JOHN KATKO, New York *(ex officio)*

LISA CANINI, *Subcommittee Staff Director*
ERIC HEIGHBERGER, *Minority Subcommittee Staff Director*
GEREMIAH LOFTON, *Subcommittee Clerk*

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

BONNIE WATSON COLEMAN, New Jersey, *Chairwoman*

DONALD M. PAYNE, JR., New Jersey
DINA TITUS, Nevada
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
BENNIE G. THOMPSON, Mississippi *(ex officio)*
CARLOS A. GIMENEZ, Florida, *Ranking Member*
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
JOHN KATKO, New York *(ex officio)*

ALEX MARSTON, *Subcomittee Staff Director*
KATHRYN MAXWELL, *Minority Subcomittee Staff Director*
ALICE HAYES, *Subcomittee Clerk*

CONTENTS

ASSESSING THE DEPARTMENT OF HOMELAND SECURITY'S EFFORTS TO COUNTER UNMANNED AIRCRAFT SYSTEMS

Thursday, March 31, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON OVERSIGHT, MANAGEMENT, AND ACCOUNTABILITY, AND THE
SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY,
Washington, DC.

The subcommittees met, pursuant to notice, at 10 a.m., in room 310, Cannon House Office Building, Hon. J. Luis Correa [Chairman of the Subcommittee on Oversight, Management, and Accountability] presiding.

Present from the Subcommittee on Oversight, Management, and Accountability: Representatives Correa, Payne, Titus, Torres, Jackson Lee, Meijer, Bishop, and Harshbarger.

Present from the Subcommittee on Transportation and Maritime Security: Representatives Watson Coleman, Gottheimer, Luria, Gimenez, Van Drew, Norman, Miller-Meeks, and Guest.

Chairman CORREA. The Subcommittees on Oversight, Management, and Accountability, and Transportation and Maritime Security will now come to order. Without objection, the Chair is authorized to declare the subcommittees in recess at any time.

Let me start by thanking everyone for joining us today. I would like to thank Chairwoman Watson Coleman and Ranking Member Gimenez of the Transportation and Maritime Security Subcommittee for coming together with Ranking Member Meijer and me to hold this very important hearing.

We are here today to discuss the Department of Homeland Security's use of its authority to mitigate threats posed by drones. This authority to counter unmanned aircraft systems, known as C–UAS authority, was granted by Congress to the Department of Homeland Security in 2018.

Since then, drone use has only increased in popularity and skies above our country have never been more crowded. While many of these drones are operated by hobbyists, photographers, and journalists who pose no threat to the American people, the technology has also been used by malicious actors who seek to compromise homeland security in a number of ways.

Most frequently, these threats have taken the form of surveillance, undermining law enforcement missions and the smuggling of

narcotics and other illicit materials. There is also the potential for drones to carry an explosive payload to target either persons or facilities. Even drone operators who pose no malicious threat may inadvertently threaten or cause dangerous interference around airports, natural disaster sites, and sporting events.

There is no denying that with the increasing availability and use of these unmanned aircraft systems, we must be able to respond quickly and effectively to any immediate security threat. However, with all missions the Department undertakes, the response to these threats must be Constitutionally protected, establishing and protecting for privacy, civil rights, and civil liberties.

For example, civil liberties groups have raised concerns that freedom of the press may be at risk since DHS can limit journalists from flying drones above protests or natural disaster sites, areas that there is a strong public interest in providing information to our constituents. Additionally, the groups point out the conflicts with the right of due process. For example, if a drone hobbyist inadvertently crosses the invisible line that is restricted space, their private property can and will be seized without the approval of a judge.

Privacy, civil rights, and civil liberties protections are the cornerstone of our democracy. As DHS grapples with the very real threat posed by drones, we must be constantly on guard to make sure that civil rights, our democracy, is protected. It is a fine line for the Department to walk, and engagement from DHS Offices of Privacy and Civil Rights and Civil Liberties to oversee the use of this authority is important in this process.

Today, we look forward to hearing more about how the Department has worked with these offices and walks the line between mitigating threats and protecting the rights every American citizen has. With the Government's C–UAS authority set to expire in October, we have a tremendous opportunity, a great opportunity here to examine how DHS has used its authority and thus far what changes can be needed when the committee considers reauthorization.

I look forward to hearing from our panel of witnesses today, who represent some of the Department components that are most actively engaged in C–UAS or drone activity.

[The statement of Chairman Correa follows:]

STATEMENT OF CHAIRMAN J. LUIS CORREA

MARCH 31, 2022

We're here to discuss the Department of Homeland Security's use of its authority to mitigate threats posed by drones. This authority to counter unmanned aircraft systems, known as C–UAS authority, was granted by Congress to the Department of Homeland Security, among others, in 2018.

Since then, drone use has only increased in popularity and the skies above our country have never been more crowded. While many of these drones are operated by hobbyists, photographers, and journalists who pose no threat to the American people, the technology has also been used by malicious actors who seek to compromise homeland security in a variety of ways.

Most frequently, these threats have taken the form of surveillance undermining a law enforcement mission, and the smuggling of narcotics and other illicit materials. There is also the potential for drones to carry an explosive payload to a targeted person or facility. Even drone operators who pose no malicious threat may in-

advertently cause dangerous interference around airports, natural disaster sites, and sporting events.

There can be no denying that with the increasing availability and use of these unmanned aircraft systems, DHS must be able to respond quickly and effectively to any immediate security threat. However, as with all missions the Department undertakes, the response to this threat must respect Constitutionally-established protections for privacy, civil rights, and civil liberties.

For example, civil liberties groups have raised concerns that freedom of the press is at risk since DHS could limit journalists from flying drones above protests or natural disaster sites—areas where there is a strong interest in providing information to the public. Additionally, the groups point out conflicts with the right to due process. If a drone hobbyist, for example, inadvertently crosses an invisible line that is restricted airspace, their private property can be seized without approval from a judge.

Privacy, civil rights, and civil liberties protections are the cornerstone of our democracy. As the Department grapples with the very real threat posed by drones, there must be guardrails for those who mean no harm. It is a fine line for the Department to walk, and engagement from the DHS Offices of Privacy and Civil Rights and Civil Liberties to oversee the use of this authority is a vital part of the process.

Today, I look forward to hearing more about how the Department has worked with these offices and walks the line between mitigating threats and protecting the rights every American citizen is afforded.

With the Government's C–UAS authority set to expire in October, we have the opportunity to examine how DHS has used its authority thus far and what changes may be needed when the committee considers reauthorization.

I look forward to hearing from our panel of witnesses today, who represent some of the Department components that are most actively engaged on C–UAS.

Chairman CORREA. With that, I thank all of you for joining us today. The Chair now recognizes the Ranking Member of this committee, the gentleman from Michigan, Mr. Meijer, for his opening comments.

Mr. MEIJER. Thank you, Chairman Correa, Chairwoman Watson Coleman, and Ranking Gimenez for holding this hearing. I also want to thank our witnesses for joining us to talk about unmanned aircraft systems.

Unmanned aircraft systems, commonly known as drones, are becoming a ubiquitous part of our lives. Just like any other technology, they can be used for both good and bad ends. Just within the Department of Homeland Security, but along with other Government agencies, we use UAS to support firefighting and search-and-rescue operations, to support disaster relief, but also to help secure our borders.

But as the commercial market for UAS continues to expand, there is an increased threat posed by these drones. Commercial drones, as we have seen, can threaten our airports, our critical infrastructure, and high-profile events, whether intentionally or accidentally. To address this growing threat Congress passed the Preventing Emerging Threats Act of 2018 to give DHS the authority to protect certain assets where there is a National security risk posed by drones.

However, the authorities in this legislation do not cover such areas as large domestic airports. The bill also required DHS to assess current Federal, State, and local authorities to counter this threat.

I have to point out that DHS's report, which the committee received just a few months ago, is 2½ years late. For an authority that was intensely negotiated among the interagency as well as

various Congressional committees of jurisdiction, such delinquency is unacceptable.

Nevertheless, the report found that State and local law enforcement entities are extremely limited in what they can do to counter the threats posed by UAS because of laws put in place to protect, importantly, citizens' privacy. Specifically, Federal laws such as the Wiretap Act of 1968 and the Computer Fraud and Abuse Act of 1986, while still relevant and important in the fight to protect civil liberties, were passed long before drones were commonplace or even on the periphery of our imaginations. These laws effectively limit who can respond to UAS incident and how. Specifically, current statute makes it illegal for State and local law enforcement to intercept communications or access a computer without authorization. While these are necessary steps to take to counter a threatening drone, the existing restrictions on local law enforcement make it nearly impossible to track down the operator of such a drone.

Furthermore, many of our critical infrastructure sites are privately owned and their owners are responsible for the protection of these facilities. The United States has 16 critical infrastructure sectors whose assets and networks are so vital that any damage or destruction to them could have a debilitating effect on our National and economic security. Despite the importance of these facilities, their owners also lack legal authorities to buy and operate counter-drone technologies to protect against a threatening UAS.

Today we need to examine carefully the restrictions caused by previous legislation in addition to the lack of clearly-defined authorities which has resulted in a quagmire of laws that Federal, State, and local law enforcement agencies are at risk of violating if they attempt to interfere with a threatening drone.

This problem is substantial when we consider that terrorists and criminals promote the use of drone technology for illicit means. These groups can buy commercial drones to carry and drop explosive payloads, smuggle drugs, and conduct surveillance.

I know that just last week Chief Border Patrol Agent Brian Hastings used technology to counter-surveil drug smugglers. The smugglers were using a drone to scout areas for law enforcement before sending bundles of drugs across the border, so effective means of opposition ISR.

Thanks to Border Patrol's ability to use counter-UAS technology they were able to seize over 600 pounds of marijuana. I am curious to hear how frequent this type of occurrence is and whether they have increased over the past 5 years with the proliferation of off-the-shelf drones.

Congress has put forward some legislation to address this threat. For example, to prevent terrorists from using drones for nefarious purposes I cosponsored with Representative McCaul, the Ranking Member on Foreign Affairs, the Stop Iranian Drones Act to prevent Iran and Iranian-aligned terrorist organizations and militia groups from buying commercial drones and parts to use in attacks against the United States and allied nations. This type of legislation is a step in the right direction, but there is far more to do.

But I am looking forward to hearing today from all of you, specifically from DHS, on two things. First, I want to know what DHS

is doing to work with other Federal agencies and State and local law enforcement partners to mitigate drones and how effective this coordination has been. Second, to hear what DHS needs based on the demonstrated experience with UAS, particularly on our Southern Border, to mitigate this threat more effectively.

Given that the authorities granted in this act expire in October, we need now to decide how and to what extent we should move forward with these authorities. To that end I think DHS needs to make its case on whether Congress should renew these authorities, should modify them, extend them, because as of right now, I don't think we have made that case yet. But I am hopeful that DHS can provide clarity and can help us improve the handling of new authorities granted by Congress for evolving threats to homeland security.

Thank you again to the Chairs, the Ranking Member, and the witnesses. With that, Mr. Chairman, I yield back.

[The statement of Ranking Member Meijer follows:]

STATEMENT OF RANKING MEMBER PETER MEIJER

Thank you, Chairman Correa, Chairwoman Watson Coleman, and Ranking Member Gimenez, for holding this hearing. I also want to thank our witnesses for joining us to talk about unmanned aircraft systems (UAS).

Unmanned Aircraft Systems (UAS), commonly known as "drones," are becoming a ubiquitous part of our lives. Just like any other technology, they can be used to good and bad ends. The Department of Homeland Security and other Government agencies use UAS to:

- support firefighting and search-and-rescue operations,
- to provide disaster relief, and
- to help secure our borders.

But, as the commercial market for UAS continues to expand, there is an increased threat posed by drones. Commercial drones can threaten our airports, our critical infrastructure, and high-profile events, whether intentionally or accidentally.

To address this growing threat, Congress passed the Preventing Emerging Threats Act of 2018. This Act gave DHS the authority to protect certain assets when there is a National security risk posed by drone. However, the authorities in this legislation did not cover such things as large, domestic airports.

The bill also required DHS to assess current Federal, State, and local authorities to counter this threat. I have to point out that DHS's report, which the committee just received a few months ago, is 2½ years late. For an authority that was intensely negotiated among the interagency, as well as various Congressional committees of jurisdiction, such delinquency is absolutely unacceptable. Nevertheless, the report found that State and local law enforcement entities are extremely limited in what they can do to counter threats posed by UAS because of laws that were put in place to protect citizens' privacy. Specifically, Federal laws such as the Wiretap Act of 1968 and the Computer Fraud and Abuse Act of 1986, while still relevant, were passed long before drones were commonplace.

These laws effectively limit who can respond to a UAS incident and how. Specifically, current statute makes it illegal for State and local law enforcement to intercept communications or access a computer without authorization. These are necessary steps to take to counter a threatening drone, yet the existing restrictions on local law enforcement make it nearly impossible to track down the operator of a drone.

Furthermore, many of our critical infrastructure sites are privately owned, and their owners are responsible for protecting these facilities. The United States has 16 critical infrastructure sectors whose assets and networks are so vital that any damage or destruction to them could have a debilitating effect on our National and economic security. Despite the importance of these facilities, their owners also lack the legal authority to buy and operate counter drone technologies to protect against a threatening drone.

Today, we need to examine carefully the restrictions caused by previous legislation in addition to the lack of clearly defined authorities that has resulted in a quagmire of laws that Federal, State, and local law enforcement agencies are at risk of breaking if they attempt to interfere with a drone.

This problem is substantial when we consider that terrorists and criminals promote the use of drone technology for illicit means. These groups can buy commercial drones to carry and drop explosive payloads, smuggle drugs, and conduct surveillance. I know that just last week, Chief Border Patrol Agent Brian Hastings used technology to counter surveil drug smugglers. The smugglers were using a drone to scout areas for law enforcement before sending bundles of drugs across the border. Thanks to Border Patrol's ability to use counter UAS technology, it was able to seize over 600 lbs. of marijuana. I'm curious to hear how frequent this type of occurrence is and whether they have increased over the past 5 years.

Congress has put forward some legislation to address this threat. For example, to prevent terrorists from using drones for nefarious purposes, I cosponsored Representative McCaul's Stop Iranian Drones Act. This bill will prevent Iran and Iranian-aligned terrorist and militia groups from buying commercial drones and parts that can be used in attacks against the United States and our partner nations.

This type of legislation is a step in the right direction, but we need to do better.

I'm looking forward to hearing from all of you on this. Specifically, I'd like to hear from DHS on 2 things:

- First, I want to know how DHS works with other Federal agencies, and State and local law enforcement partners, to mitigate drones and how effective this coordination is.
- Second, I want to hear what DHS needs, based on its experience with drones, particularly at our Southern Border, to mitigate them more effectively.

Given that the authorities granted in the Act expire in October, we need to decide how—and to what extent—we should move forward with these authorities. To that end, I think DHS needs to make its case on whether Congress should renew these authorities. As of now, I don't think DHS has done so, but I am hopeful that DHS can provide us some clarity and can improve its handling of new authorities granted by Congress for evolving threats to homeland security.

Thank you again, to the Chairs, the Ranking Member, and the witnesses, and I yield back.

Chairman CORREA. Thank you, Mr. Meijer. The Chair now recognizes the Chairwoman of the Subcommittee on Transportation and Maritime Security, the gentlewoman from New Jersey, Mrs. Watson Coleman, for her opening statement.

Chairwoman WATSON COLEMAN. Thank you very much, Mr. Chairman. Thank you to all of our witnesses for joining us today for this critical and timely discussion.

In 2018, Congress granted DHS and DOJ unlimited authority to mitigate drones posing critical threats to specific facilities or, in other words, to engage in what we call C–UAS. This authority expires in the fall and it falls to Congress to determine whether to reauthorize, eliminate, or reform it. As October approaches, it is imperative that we open up this important conversation to the public, and privacy and civil liberties stakeholders in particular, through forums such as this hearing.

For years DHS, together with DOJ and FAA, has briefed this committee on the threats that militias and unauthorized drones pose to the homeland. Though we can't discuss everything we have learned in this setting, we know the threats are real.

Drones are cheap to produce and purchase. Operators, whether malicious or unwitting, can cause major problems when they fly drones into restricted airspaces.

Drones wreaked havoc upon Gatwick Airport in London for a few days in 2018, causing thousands of flight cancellations. In my home State of New Jersey, air traffic at the Newark Liberty International Airport was shut down for an hour-and-a-half when drones breached its protect airspace in 2019.

We have seen drones interrupt sporting events and cause disruption. One could imagine drones facilitating more serious harm to our Nation's security, whether through hostile surveillance of sen-

sitive Government facilities or critical infrastructure or even used in kinetic attacks.

As drones become more ubiquitous and more advanced, these risks are only going to grow. According to the FAA, there are currently 850,000 registered drones in the United States, including 300,000 commercial drones and 500,000 recreational drones.

To be clear, drones provide many benefits to society. Journalists are using drones to cover the news. Hobbyists are using drones to enjoy their weekends. Businesses and governments are using them to inspect infrastructure, survey land, and monitor crops.

As with all new technologies, we can't focus just on the risks or the benefits. We need to balance both. In this spirit, I do have some questions about Section 124n, the Government's C–UAS authority as it is currently constructed.

When we create limited exceptions to laws like the wiretap, as this authority does, we must consider fundamental principles, like privacy and due process. When we place limits on the use of a technology, like drones that journalists use every day to cover protests, natural disasters, and other matters of core public interest, as this authority does, we must consider the First Amendment of the Constitution and the freedom of the press.

That means that we need a clear understanding of how DHS is interpreting key terms in the statute and ensuring the statute's First and Fourth Amendment protections are held. We must ask ourselves as we look forward what more can we do to ensure privacy and civil liberty unions' protections are baked in at every level of DHS's C–UAS planning and operations?

While I am looking forward to hearing from our witnesses about the real threats posed by drones as well as DHS's response to these threats, I am equally eager to learn about the Department's approach on questions of privacy and civil liberties.

Homeland security may be about protecting our Nation's critical assets, but there is no asset more critical than our values. I look forward to engaging in this public conversation as we work to determine an appropriate path forward on these issues.

I want to thank our witnesses for joining us as well as for their efforts to ensure our Nation is prepared for the long list of drone-related threats that we may face.

I yield back.

[The statement of Chairwoman Watson Coleman follows:]

STATEMENT OF CHAIRWOMAN BONNIE WATSON COLEMAN

MARCH 31, 2022

In 2018, Congress granted DHS and DOJ a limited authority to mitigate drones posing critical threats to specific facilities. Or in other words, to engage in what we call C–UAS. This authority expires in the fall—and it falls to Congress to determine whether to reauthorize, eliminate, or reform it. As October approaches, it is imperative that we open up this important conversation to the public—and privacy and civil liberties stakeholders in particular—through forums such as this hearing.

For years, DHS, together with DOJ and FAA, has briefed this committee on the threats that malicious and unauthorized drones pose to the homeland. Though we can't discuss everything we've learned in this setting, we know the threats are real. Drones are cheap to produce and purchase, and operators, whether malicious or unwitting, can cause major problems when they fly drones into restricted airspaces.

Drones wreaked havoc upon Gatwick Airport in London for a few days in 2018, causing thousands of flight cancellations, and in my home State of New Jersey, air

traffic at Newark Liberty International Airport was shut down for an hour-and-a-half when drones breached its protected airspace in 2019.

We've seen drones interrupt sporting events and cause disruption. And one could imagine drones facilitating more serious harm to our Nation's security, whether through hostile surveillance of sensitive Government facilities or critical infrastructure, or even use in kinetic attacks.

As drones become more ubiquitous and more advanced, these risks are only going to grow. According to the FAA, there are currently 850,000 registered drones in the United States, including 300,000 commercial drones and 500,000 recreational drones. To be clear, drones provide many benefits to society. Journalists are using drones to cover the news. Hobbyists are using drones to enjoy their weekends. Businesses and governments are using them to inspect infrastructure, survey land, and monitor crops.

As with all new technologies, we can't focus just on the risks or the benefits. We need to balance both. In this spirit, I do have some questions about Section 124n—the Government's C–UAS authority—as it is currently constructed. When we create limited exceptions to laws like the Wiretap Act—as this authority does—we must consider fundamental principles like privacy and due process.

When we place limits on the use of a technology like drones that journalists use every day to cover protests, natural disasters, and other matters of core public interest—as this authority does—we must consider the First Amendment of the Constitution and the freedom of the press.

That means we need a clear understanding of how DHS is interpreting key terms in the statute and ensuring the statute's First and Fourth Amendment protections are upheld. And we must ask ourselves, as we look forward: What more can we do to ensure privacy and civil liberties protections are baked-in at every level of DHS's C–UAS planning and operations?

While I am looking forward to hearing from our witnesses about the real threats posed by drones, as well as DHS's response to these threats, I am equally eager to learn about the Department's approach on questions of privacy and civil liberties. Homeland security may be about protecting our Nation's critical assets, but there is no asset more critical than our values.

I look forward to engaging in this public conversation as we work to determine an appropriate path forward on these issues. I want to thank our witnesses for joining us, as well as for their efforts to ensure our Nation is prepared for the long list of drone-related threats we face.

Chairman CORREA. Thank you, Madam Chair. The Chair now recognizes the Ranking Member of the Subcommittee on Transportation and Maritime Security, the gentleman from Florida, Mr. Gimenez, for an opening statement. Welcome, sir.

Mr. GIMENEZ. Thank you. Thank you, Chairman Correa, Chairwoman Watson Coleman, and Ranking Member Meijer for holding this hearing today.

The number of unmanned aircraft systems, commonly known as drones, in our Nation's airspace is increasing. Their technical capabilities are continually improving. The evolving threat of drones used by unknown or maligned actors present a challenge in keeping our country's transportation systems, critical infrastructure, and borders secure.

In 2018, reports of drone sightings near the runways of London's Gatwick Airport caused the cancellation of 1,000 flights over the Christmas holidays, negatively impacting about 140,000 passengers and resulting in a significant economic impact. In the United States this year, there have already been two commercial flights whose pilots were forced to take evasive action to avoid collision with a drone.

DHS is currently testing technology to detect and track and identify drones entering restricted airspace. Last year I was pleased to visit the TSA test bed at my home airport of Miami International. I look forward to hearing from today's witnesses on how security

and surveillance technology can be used at airports and surface transportation sites Nation-wide to protect the traveling public.

The number and sophistication of drones at the Southwest Border has also increased over the last several years. I am particularly concerned that transnational criminal organizations are using drones to move migrants and narcotics across the border and conduct surveillance on Customs and Border Protection personnel. It appears that the use of drones for illicit border activity is widespread and it is a critical element of these groups' operations.

I thank the witnesses for being here today to discuss what capabilities DHS is using to counter drones through the authorities Congress gave them in the Preventing Emerging Threats Act of 2018. Thank you, Chairman and Madam Chairwoman, and I yield back the balance of my time.

[The statement of Ranking Member Gimenez follows:]

STATEMENT OF RANKING MEMBER CARLOS GIMENEZ

Thank you, Chairman Correa, Chairwoman Watson Coleman, and Ranking Member Meijer for holding this hearing today.

The number of unmanned aircraft systems, commonly known as drones, in our Nation's air space is increasing and their technical capabilities are continuously improving. The evolving threat of drones used by unknown or malign actors present a challenge in keeping our country's transportation systems, critical infrastructure, and borders secure.

In 2018, reports of drone sightings near the runway at London's Gatwick airport caused the cancellation of 1,000 flights over the Christmas holiday, negatively impacting 140,000 passengers and resulting in a significant economic impact. In the United States this year, there have already been two commercial flights whose pilots were forced to take evasive action to avoid collision with a drone.

DHS is currently testing technology to detect, track, and identify drones entering restricted airspace. Last year, I was pleased to visit the TSA test bed at my home airport of Miami International. I look forward to hearing from today's witnesses on how security and surveillance technology can be used at airports and surface transportation sites Nation-wide to protect the traveling public.

The number and sophistication of drones at the Southwest Border has also increased over the last several years. I'm particularly concerned that transnational criminal organizations are using drones to move migrants and narcotics across the border and conduct surveillance of Customs and Border Protection (CBP) personnel. It appears that the use of drones for illicit cross border activity is wide-spread and a critical element of these groups' operations.

I thank the witnesses for being here today to discuss what capabilities DHS is using to counter drones through the authorities Congress gave them in the Preventing Emerging Threats Act of 2018.

Thank you, Chairman and Madame Chairwoman, and I yield back the balance of my time.

Chairman CORREA. Members are reminded that the committee will operate according to the guidelines laid out by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures. Without objection, Members on the subcommittee shall be permitted to sit and question the witnesses. Additional Member statements may be submitted for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

MARCH 31, 2022

In 2018, Congress granted the Department of Homeland Security and the Department of Justice limited authority to counter the threat posed by unmanned aircraft systems. That authority is set to expire this October, leaving this committee respon-

sible for assessing how DHS has conducted its C–UAS mission and what changes may be needed before Congress reauthorizes or reforms that authority.

Drones are more affordable and accessible than ever. From families capturing vacation memories to journalists covering major National news events, millions of Americans operate drones responsibly and safely each year. But, when used nefariously, drones can pose a great threat to public safety and National security.

Malicious actors have used drones to smuggle illicit materials across borders and into prisons and have disrupted air travel and law enforcement activities. Some drone operators just fail to understand the rules and may disrupt major public events, transportation systems, or other sensitive locations simply by accident. Whether the operator is flying innocently or maliciously, the Department must be able to respond quickly, assess the threat, and ensure any actions to mitigate a drone uphold Americans' Constitutional rights to privacy, civil rights, and civil liberties.

It is essential that we continue to protect the freedom of the press, including when journalists use drones to capture images of major news stories, whether it be destruction following a natural disaster or large protest gatherings. We must also ensure that drone operators, many of whom are merely backyard hobbyists, do not have their private property seized and destroyed by the Government for minor, accidental infractions. With that in mind, I am particularly interested in hearing from our witnesses on how, specifically, a drone threat is mitigated and what steps are taken to preserve the rights of Americans against unnecessary search and seizure.

The upcoming sunset of the Department's C–UAS authority provides Congress with an opportunity to conduct a stringent assessment of the current authority, its strengths, and its shortcomings, before choosing whether and how to reauthorize counter-drone activities.

I look forward to learning more from our witnesses, each with their own perspective on how the Department has used its C–UAS authority, about how they have grappled with responding efficiently to threats while protecting privacy and civil liberties.

Chairman CORREA. Now I would like to welcome our panelists. Our first witness is Ms. Samantha Vinograd, the acting assistant secretary for Counterterrorism and Threat Prevention at the Department of Homeland Security. She began her career as a deputy U.S. Treasury attaché to Iraq; subsequently served on the National Security Council. She was previously a CNN national security analyst, a senior advisor at the Biden Institute, and a visiting fellow at the University of Chicago Institute for Politics.

Our second witness, Rear Admiral Scott Clendenin. He served as then-U.S. Coast Guard assistant commandant for response policy. He is responsible for the U.S. Coast Guard policy in 7 operational mission areas, including defense operations and law enforcement. Before that, he served afloat for 14 years at sea on Coast Guard cutters conducting multi-mission patrols in the Atlantic, Pacific, and throughout the Caribbean.

Our third witness is Austin Gould, the acting deputy executive assistant administrator for operation support at the Transportation Security Administration. He is responsible for strengthening TSA's operational capabilities and driving mission performance through analysis and innovation. Prior to joining TSA, Mr. Gould served as a captain in the U.S. Coast Guard. During his 30-year Coast Guard career he worked in a variety of operational and acquisition management positions.

Our final witness, Mr. Dennis Michelini, deputy executive assistant commissioner of air and marine operations at Customs and Border Protection. He began his Federal law enforcement career in 1995 as a U.S. Border Patrol agent. In 2000, he became an aircraft pilot and joined AMO. From 2013 to 2016, he served as director of air operations, where he was responsible for UAS operations and

the employment of new UAS technologies throughout the CBP environment.

Deep breath. Without objection, the witnesses' full statements will be inserted into the record. Now I am going to ask each witness to summarize their statements for 5 minutes, beginning with Ms. Samantha Vinograd. Welcome, ma'am.

STATEMENT OF SAMANTHA VINOGRAD, ACTING ASSISTANT SECRETARY FOR COUNTERTERRORISM, THREAT PREVENTION, AND LAW ENFORCEMENT, OFFICE OF STRATEGY, POLICY, AND PLANS, U.S. DEPARTMENT OF HOMELAND SECURITY

Ms. VINOGRAD. Chairman Correa, Chairwoman Watson Coleman, Ranking Member Gimenez, Ranking Member Meijer, and distinguished Members of the subcommittees, thank you for inviting the Department of Homeland Security to be with you today.

I began my Government service under the Bush administration in 2007 as a civil servant at Treasury both in Iraq and Washington, DC. I subsequently served on the National Security Council in a variety of roles. I was honored to rejoin Government service last February at the Department of Homeland Security as senior counselor and later as acting assistant secretary for counterterrorism, threat prevention, and law enforcement. It has been an honor to serve bipartisan administrations on critical National security and homeland security issues affecting our country.

Let me be very clear at the outset. The Department of Homeland Security considers our C–UAS mission to be twofold: We are focused on using our authority to mitigate credible threats; No. 2, the safety and security of DHS missions. At the same time, in doing so, we are just as focused as protecting privacy and civil rights and civil liberties. I look forward to sharing with you how we are accomplishing both aspects of our C–UAS mission.

DHS is judiciously implementing the authorities that Congress granted in the Preventing Emerging Threats Act of 2018 to conduct C–UAS operations. These operations respond to the evolving and dynamic UAS threat environment and ensure that privacy and civil rights and civil liberties are protected. The Department exercises this authority to protect National security and public safety while minimizing the impact to the National airspace system.

Technological advances have accelerated UAS capabilities across commercial and recreational applications. Their compact size and often low cost make them suitable for performing a variety of beneficial mission sets. UAS play a transformative role in fields such as transport and delivery, emergency response, critical infrastructure management, agriculture, and more.

DHS supports the lawful use of UAS. We are only concerned with malicious or illicit use by threat actors. We do know that the scale and scope of UAS threats are increasing. We are deeply concerned about UAS weaponization, smuggling, surveillance, disruption, and the fostering of other illicit activities, particularly at airports and in border regions. My colleagues today will provide additional details on what we are seeing from a threat perspective and how DHS is responding.

We also know that as we look toward the future, emerging technologies will expand the boundaries of what is possible for threat actors. We are positioning ourselves to remain ahead of technology curve through dedicated research, testing, training, and evaluation efforts.

The Preventing Emerging Threats Act of 2018 grants DHS and the Department of Justice relief from several Federal criminal statutes when performing C–UAS actions identified in the act, which allows us to engaging in very specific electronic detection and electronic mitigation through intercepting the communications between a control device—a command device and the UAV itself. This authority explicitly enables the protection of designated-covered facilities or assets from credible UAS threats that relate to specific DHS mission sets. The act also authorizes DHS and DOJ to protect NSSE and SEAR events, a provision of support to State, local, Tribal, and territorial law enforcement upon the request of the chief executive officer of the respective State or territory for mass gathering that are limited to a specific time frame and location, as well as the protection of an active Federal law enforcement investigation.

DHS successfully coordinated over 250 operational C–UAS deployments and 30 research, testing, training, and evaluation events since the authorities were granted, consistent with the requirements outlined in the act. In those deployments, DHS has never caused undue interference with the National airspace. Importantly, our Privacy Office has seen no cause to implement a privacy compliance review or to engage in another form of a privacy investigation since the authority was granted.

To ensure consistent application of C–UAS authorities across the Department, DHS established a C–UAS Program Management Office. This office manages and supports C–UAS activities to ensure component alignment, DHS is a large organization, with departmental strategy and policy guidance.

This is especially important, for example, for our coordination with the FAA. The PMO has worked closely with the FAA to develop objective standards that define critical elements of coordination at the Department. Moreover, the Secretary issued DHS-wide policy guidance which requires components to establish their own internal C–UAS policies. The policy guidance establishes formal processes for components to obtain deployment authorizations.

Chairman CORREA. Ms. Vinograd, I am going to ask you to summarize and conclude your statement.

Ms. VINOGRAD. Certainly. DHS applies a multi-layered approach to promoting privacy and civil rights and civil liberties, which I will articulate today, both at the Department-wide level and the component level. We also are focused on ensuring transparency and promoting First Amendment-protected activities when we do work with the FAA to implement temporary flight restriction.

I am very honored to be with you here today and look forward to answering your questions with respect to gaps in our authorities and the way forward with respect to the threat landscape. Thank you, sir.

[The joint prepared statement of Ms. Vinograd, Mr. Clendenin, Mr. Gould, and Mr. Michelini follows:]

JOINT PREPARED STATEMENT OF SAMANTHA VINOGRAD, SCOTT W. CLENDENIN, AUSTIN GOULD, AND DENNIS J. MICHELINI

THURSDAY, MARCH 31, 2022

Chairwoman Watson Coleman, Chairman Correa, Ranking Member Gimenez, Ranking Member Meijer, and distinguished Members of the subcommittees, thank you for inviting us to testify regarding emerging threats posed by the malicious use of unmanned aircraft systems (UAS[1] or "drones"[2]) in the United States and the missions of the Department of Homeland Security (DHS) to counter such threats. DHS continues to judiciously implement the authorities Congress granted through enactment of the Preventing Emerging Threats Act of 2018 (the "Act"), codified at 6 U.S.C. § 124n, to conduct UAS detection and counter-unmanned aircraft system (C–UAS)[3] activities in response to the evolving and dynamic threat environment, while ensuring the protection of privacy and civil rights and civil liberties. The Department takes implementation of its C–UAS authorities seriously, exercising them to protect National security and public safety while preserving the rights of the public and working with the Federal Aviation Administration (FAA) to minimize impact to the National airspace system (NAS).

Technological advances have accelerated UAS capabilities across a variety of commercial and recreational applications. Their compact size and often low cost make them suitable for many beneficial applications, performing critical tasks with minimal risk and expense. A wide spectrum of domestic users—including industry, private citizens, and Federal, State, local, Tribal, and territorial governments—are using or expect to use UAS, which may play a transformative role in fields such as transport and delivery, critical infrastructure management, agriculture, search and rescue, disaster response, public safety, coastal security, military training, and others. Estimates suggest that rapidly advancing UAS technology and integration of drones into the NAS will result in new innovations and generate economic growth and opportunity for businesses and private citizens. DHS supports the lawful use of UAS, including by commercial and recreational users. Like all technology, however, UAS can be exploited for malicious use by threat actors, threatening National security and public safety, which is the major concern of DHS.

Our joint testimony today describes threats to the U.S. homeland posed by the malicious use of drones and how we use our authorities to protect against these threats. We explain our tiered approach to implementation and governance of C–UAS authorities, including compliance with existing laws and regulations, issuing Department and component-level policy guidance, and specific privacy, civil rights, and civil liberties documentation that surpasses statutory requirements. Our testimony underscores the processes required to gain Departmental approval and authorization to conduct C–UAS activities, which are designed to protect privacy, civil rights, and civil liberties, safeguard aviation safety, and ensure leadership review of every deployment. Additionally, we will provide examples of DHS components' C–UAS activities, including testing and operational deployments by the U.S. Coast Guard (USCG), Transportation Security Administration (TSA), and Customs and Border Protection (CBP). Finally, we highlight gaps in the Department's current authorities that sunset on October 5, 2022—as noted in the DHS C–UAS Assessment delivered to Congress in December 2021—and we indicate the Department's intention to request reauthorization and expansion of its C–UAS authorities to remedy such gaps to address dynamic and evolving threats.

THREATS TO THE U.S. HOMELAND FROM THE MALICIOUS USE OF UAS

The malicious use of UAS is increasing and diversifying in the United States and abroad. The threat can take several forms, including kinetic attacks with payloads of firearms, explosives, or weapons of mass destruction; the illicit trafficking of narcotics or contraband; surveillance against law enforcement; cyber attacks against wireless devices or networks; foreign intelligence; and corporate espionage or theft of intellectual property. The availability of highly-capable, low-cost UAS has led to

[1] The term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the National airspace system. See 49 U.S.C. § 44801.

[2] For the purposes of this statement, "drone" refers to the aircraft portion of a UAS.

[3] The term "counter-UAS system" means a system or device capable of lawfully and safely disabling, disrupting, or seizing control of an unmanned aircraft or unmanned aircraft system. See 49 U.S.C. § 44801. Although this term, as defined in statute, does not encompass UAS detection, references to "C–UAS" activities throughout this testimony are intended to include both UAS detection and mitigation activities.

expanded use by threat actors. This has required DHS to grow its domain awareness and response capability efforts to identify and counter smaller, more agile, and less attributable threats across its mission spaces.

We are most concerned with UAS weaponization, smuggling, surveillance, disruption, and the fostering of other illicit activity, particularly in venues where DHS already conducts its missions including airports, border regions, protective operations, National Special Security Events (NSSE), Special Event Assessment Rating (SEAR) events, and mass gatherings. Throughout border regions, CBP personnel have observed UAS used to conduct surveillance and reconnaissance of their operations and have identified a multitude of unmanned aircraft that were deemed as credible threats [4] or enabling other criminal activity such as smuggling, trafficking, and conveyance of illicit materials. At critical infrastructure, key resource sites, sensitive Government facilities, and Federal properties Nation-wide, CBP and Federal Protective Service (FPS) personnel have observed UAS operations that appear to conduct intelligence gathering, physical security observation, and strategic reserves assessments on behalf of threat actors. U.S. Secret Service (USSS) officers have identified UAS violating temporary flight restrictions put in place by the FAA to protect the President and other Government leaders, the type of threats exemplified by the assassination attempt on Venezuelan President Maduro utilizing explosives-laden drones in 2018. TSA and the Cybersecurity and Infrastructure Security Agency (CISA) continue to engage with transportation sector and critical infrastructure partners to improve stakeholder response capabilities and reaction times to UAS threats.

As we look toward the future, emerging technologies will expand the boundaries of what is possible for threat actors. Capabilities such as controlling multiple drones with one remote, autonomous flight plans, obstacle avoidance, extended communications ranges, and prolonged battery life require constant reevaluation of the Department's prevention and response tactics. Remaining adaptive and proactive in countering UAS threats as they evolve is critical to DHS in executing its missions. Through research, testing, training, and evaluation efforts (RTTE), spearheaded by the DHS Science and Technology (S&T) Directorate, and as recurring innovation and simulation efforts across the interagency mature, we are positioning ourselves to remain ahead of the technology curve.

CURRENT DHS C–UAS AUTHORITY AND ITS USE

The Act grants DHS and the Department of Justice (DOJ) relief from several Federal criminal statutes, namely from provisions of Titles 18 and 49 that generally prohibit aircraft sabotage, computer fraud and abuse, interference with the operation of a satellite, wiretapping, and use of pen registers and trap-and-trace devices, to take certain actions to detect and defeat UAS posing a credible threat. The actions authorized in the Act include electronic detection, electronic mitigation through communications signal intercept and interruption, kinetic/physical mitigation, and device seizure. This authority expressly enables the protection of designated "covered facilities or assets"[5] from credible UAS threats that relate to specific DHS mission sets, including those covered by CBP, FPS, USCG, and USSS. The Act also authorizes protection of shared DHS and DOJ mission sets including protection of NSSE and SEAR events, a provision for support to State, local, territorial, or Tribal law enforcement (upon request of the chief executive officer of the respective State or territory) for mass gatherings that are limited to a specific time frame and location, and the protection of an active Federal law enforcement investigation, emergency response, or a security function that is limited to a specified time frame and location.

Consistent with requirements outlined in the Act and in coordination with the FAA, DHS successfully coordinated 246 operational C–UAS deployments and 30 RTTE events since the authorities were granted. We continue to collaborate closely

---

[4] Defined by the Secretary of Homeland Security as, "The reasonable likelihood that a UAS or unmanned aircraft activity, if unabated, would: (i) Inflict or otherwise cause physical harm to a person; (ii) inflict or otherwise cause damage or harm to assets, facilities or systems; (iii) interfere with the operational mission, including movement, security, and protection, of a covered facility or asset; (iv) facilitate unlawful activity; (v) conduct unauthorized surveillance or reconnaissance; or (vi) result in unauthorized access to, or disclosure of, classified, sensitive or otherwise lawfully protected information."

[5] Defined in the Preventing Emerging Threats Act as any facility asset that is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Secretary or the Attorney General, in coordination with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment; is located within the United States; and directly relates to an authorized DHS mission, or authorized joint DHS or DOJ mission, See 6 U.S.C. § 124n(k)(3).

with the FAA on each deployment to minimize potential impact to the NAS. By partnering with interagency colleagues such as DOJ, Department of Defense (DOD) Joint C–UAS Office (JCO), and North American Aerospace Defense Command (NORAD), our understanding of UAS activity across all domestic environments is maturing, enhancing our ability to differentiate malicious activity from authorized flights, counter credible UAS threats, and share relevant information and data. We see these collaborations and open communication channels as a foundation of shared success to protect the homeland.

POLICY AND GUIDANCE GOVERNING DHS'S USE OF C–UAS AUTHORITIES

To ensure consistent application of C–UAS authorities across all components, DHS established a C–UAS Program Management Office (PMO) within the Office of Strategy, Policy, and Plans (PLCY). The PMO manages and supports C–UAS activities to ensure component alignment with Departmental strategy and policy guidance and serves as a single point of contact for interagency partners.

This is especially true for coordination with the FAA. The PMO has worked closely with the FAA to develop an agreed-upon set of objective standards that define critical elements of coordination at the Department level, component level, and operational deployment level. Due to the sensitivities of deploying and operating C–UAS equipment and legal implications associated with relief from provisions of Titles 18 and 49 through the Act, it is imperative to have formal and streamlined C–UAS governance and communication structures in place. Objective standards ensure DHS maintains compliance with existing laws and regulations.

We recognize the critical importance of maintaining the safety and security of the NAS and coordinate with the FAA to develop repeatable processes for safe and efficient deployments of C–UAS technology. The resulting objective standards create consistency across all DHS components by establishing common definitions, guidelines for conducting risk-based assessments, including coordination with the FAA for assessments of the impact to nearby airport communications and aircraft navigation devices, reporting protocols when C–UAS equipment is "activated" or "transmitting," data retention standards and assessment of the need for other airspace protections, such as flight restrictions.

In addition to these agreed-upon objective standards, the Secretary issued the DHS C–UAS Policy Guidance on September 10, 2019 requiring DHS components to establish their own internal C–UAS policies, conduct assessments to document the protection of privacy, civil rights, and civil liberties, and develop operational plans for each unique C–UAS deployment, among other requirements.

PROCESS FOR AUTHORIZING THE USE OF C–UAS AUTHORITIES

Recognizing the complexity and nuances associated with deploying C–UAS equipment domestically, the DHS Secretary's C–UAS Policy Guidance establishes formal processes for obtaining C–UAS deployment authorizations. Major process steps include DHS components identifying a "covered facility or asset" to be designated, coordinating with FAA so they may assess potential impacts to the NAS and evaluate the need and regulatory basis for establishing flight restrictions, and receiving authorization from the Secretary to conduct C–UAS activities pursuant to the Act.

All deployments require components to conduct a risk-based assessment prior to requesting the statutorily required designation of a "covered facility or asset" from the Secretary. This assessment includes an evaluation of traditional risk elements such as threat, vulnerability, and consequence but also considers collateral risk that C–UAS systems pose to the NAS. DHS provides the FAA with C–UAS equipment operating frequencies so the FAA may evaluate potential interference with nearby airport communications or aircraft avionics (radio frequency spectrum deconfliction). When deconfliction is complete and the FAA has reviewed the operating plan, DHS and the FAA sign a coordination memorandum indicating required coordination steps are complete. The Secretary then designates the requested facility or asset as a "covered facility or asset" and authorizes the component to take C–UAS actions pursuant to the Act.

DHS and FAA coordinated these processes to enable the FAA to ensure deployments do not negatively impact the NAS, to provide details on how authorities are used, and to ensure senior leadership visibility and concurrence with operations. We work collaboratively with the FAA to successfully protect a wide range of areas, events, and mass gatherings from UAS threats and continuously review our processes and protocols to streamline tasks where possible.

HOW PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES ARE PROTECTED DURING C–UAS ACTIVITIES

DHS is committed to protecting the security of the Nation and its values. Those values include respecting the civil rights, civil liberties, and personal privacy of its citizens and visitors, as well as conducting operations with openness and accountability.

Understanding how C–UAS equipment works is essential to considering the privacy, civil rights, and civil liberties implications of its use. While drones generally operate on the same frequencies used by publicly available communication networks such as cellular, Bluetooth, and wi-fi, they use an individual network created between the drone and a controller. Some C–UAS equipment DHS uses identifies those communication networks and determines that the link is between a drone and its controller. DHS is unable to access other content on the operator's phone or device if it is being used to control the drone.

In general, the term "mitigation" involves an interruption of the signal from the drone operator's controller to the drone itself. An interruption causes the drone to enter into its pre-programmed recovery protocol, which is often to fly to its pre-designated "home" location or to simply hover in place. In cases where sending a drone "home" does not decrease the threat, some C–UAS equipment emulates a controller, thereby overpowering the signals from the operator's controller and allowing the C–UAS equipment operator to send the drone to a new "home" location or a DHS-preferred render safe location. Of import, C–UAS equipment is not constantly transmitting in the radio frequency spectrum; rather, it is generally only transmitting for seconds at a time, and only on the rare occasion when a mitigation action is under way.

The Act includes strong privacy protections. Authorized DHS components may intercept or acquire command and control (C2) communications to or from a UAS, as an exercise of DHS C–UAS authority, but only to the extent necessary to support C–UAS actions authorized by the Secretary. DHS components may only intercept, acquire, access, maintain, or use communications to or from a UAS in a manner consistent with the First and Fourth Amendments to the Constitution and other applicable Federal laws and Department policies. In addition to those privacy protections in the Act, the Department applies Section 222 of the Homeland Security Act of 2002 (as amended) to require all component C–UAS programs to submit a Privacy Threshold Assessment (PTA) and obtain Privacy Office approval prior to deploying C–UAS technology. The Privacy Office uses the PTA to determine the need for a Privacy Impact Assessment (PIA), which includes measures to mitigate privacy risks. DHS published multiple C–UAS PIAs for public consumption consistent with requirements outlined in the Homeland Security Act of 2002.

We continue to protect privacy, civil rights, and civil liberties by ensuring that RTTE activities collect only information authorized by law and needed to identify and address UAS threats. Component policies include measures to respect the lawful use of UAS without compromising the protection of a "covered facility or asset." Additionally, we developed procedures and incorporated them into Departmental and component-level policy guidance and operational plans to ensure consistency in C–UAS information handling. PLCY issued detailed guidance for developing UAS communication collection, retention, and sharing procedures, as well as addressing privacy, civil rights, and civil liberties considerations to components as an annex to the DHS Secretary's C–UAS Policy Guidance. These policies are currently undergoing review and revision consistent with lessons learned.

The FAA is a great partner for DHS, supporting the Department's efforts to protect "covered facilities or assets" while preserving access to the airspace for those operating UAS compliantly. When DHS requests temporary flight restrictions (TFRs) to accompany C–UAS activities, the FAA notifies the public of restrictions and provides the means to request a waiver should they have a legitimate need to participate in protected First Amendment activities. Additionally, by collaborating with the FAA to determine if temporary flight restrictions are needed, coordinate waiver requests within the flight restricted area, and issue notices to the public, we ensure those operating UAS compliantly in the area understand the limitations and potential actions that can be taken should they violate airspace restrictions.

EXAMPLES OF DHS COMPONENTS' C–UAS ACTIVITIES, TESTING, AND OPERATIONAL DEPLOYMENTS [6]

United States Coast Guard (USCG)

The USCG has safeguarded the American people and promoted National security, border security, and economic prosperity in a complex and evolving threat environment for over 230 years. As the principal Federal agency responsible for maritime safety and security in U.S. ports and inland waterways and along more than 95,000 miles of U.S. coastline, the USCG works collaboratively with relevant stakeholders to combat threats to the homeland and critical infrastructure, and the novel threats posed by UAS are increasingly concerning to USCG leaders.

From 2017 through 2021, the USCG observed a significant increase in suspicious UAS sightings over/near maritime assets and facilities, such as refineries and ferry/cruise ship terminals. Over the same period, UAS interfered with or crashed into USCG assets, ferries, cruise ships, and commercial vessels over 80 times. Since the enactment of the Act, the USCG conducted 26 separate C–UAS events requiring FAA approval, including 2 NSSEs and 5 SEAR events.

Currently, there are no flight restrictions over commercial maritime critical infrastructure, and owners and operators at those facilities consistently express their concern about threats posed to facilities by UAS. The USCG views the ability for these critical infrastructure facilities to obtain flight restrictions as an important step in securing the airspace in the maritime and port environments and is working with the FAA to address these concerns.

In preparation for C–UAS operations, the USCG conducts an event-specific review of privacy documentation, including any relevant PIAs, to measure the sufficiency of protocols to ensure civil liberties and privacy rights of those individuals affected by C–UAS operations. The USCG also collaborates closely with the FAA so the FAA may assess potential impacts on the NAS and the need for a temporary flight restriction and potentially issue public notices advising UAS operators and the public of the location and time period when restrictions are in place.

In addition, the USCG coordinates all C–UAS activities with the FAA, the C–UAS PMO, and other relevant law enforcement stakeholders to ensure appropriate frequency and spectrum management protocols are followed.

Transportation Security Administration (TSA)

Since its creation following the attacks on September 11, 2001, the TSA has dedicated itself to strengthening our Nation's transportation systems while ensuring freedom of movement for people and commerce. Drones are one of the latest threats to TSA's mission, and developing ways to deter and prevent potential harm from malicious activity to aviation and other transportation system sectors is one of TSA's top priorities.

In December 2018, reports of UAS sightings close to the runway at London's Gatwick Airport caused the cancellation of 1,000 flights over the Christmas holiday, adversely affecting approximately 140,000 passengers and resulting in severe economic impacts. The UAS operators were never apprehended and the resulting 36 hours of halted commercial air traffic and cascading international aviation system impacts illustrates the significant effects an unauthorized UAS can have on the surrounding airspace. Since the Gatwick incident, the number of UAS sightings reported increased every year, with the TSA receiving almost 1,900 reports of drones operating near airports in 2021, more than double the amount reported in 2020. Already this year, two commercial pilots took evasive action to avoid a drone collision: Air France Flight 007 departing New York for Paris and Sunset Aviation Flight 283 arriving in Atlanta from Orlando.

While TSA's mission is not explicitly called out in the Act, DHS, including TSA, is prepared to protect airports pursuant to the Act's authority to use C–UAS for the protection of an active Federal law enforcement investigation, emergency response, or security function, that is limited to a specified time frame and location. TSA requires every airport Federal Security Director (FSD) to develop and update a Tactical Response Plan (TRP) to support detection, tracking, identification, and in the event of a persistent threat and upon the emergency direction of the Secretary, mitigation of UAS threats at airports. The TRP documents TSA's preparation and response measures to address both errant and malicious UAS activity at and around the airport. FSDs conduct annual C–UAS exercises to test these plans with participation from State, local, Tribal, and territorial partners including airport authorities

[6] The USSS and FPS have also conducted C–UAS deployments, but those deployments are not summarized in this written testimony.

and other Federal agencies, such as the FAA and the Federal Bureau of Investigation (FBI).

TSA also established a UAS Threat and Vulnerability Assessments Unit to conduct comprehensive UAS-specific Joint Vulnerability Assessments (JVAs) at airports most at risk from errant or malicious UAS incidents. TSA uses these UAS JVAs to refine TRPs, define site-specific response plans, work with airport authorities and law enforcement partners to improve information-sharing procedures, and recommend courses of action for the future. Since February 2021, TSA conducted 17 full UAS-specific JVAs.

Looking to the future, TSA established technology test beds at Miami International Airport and Los Angeles International Airport and is evaluating UAS detection technology for operational effectiveness in the airport environment, in coordination with DHS S&T and the FAA. TSA tests a range of technologies at the sites, including radar, thermal imaging, and electro-optical cameras. TSA uses a continuous technology testing cycle in its UAS test beds to keep up with the rapidly-evolving UAS technology market and meet the needs of the interagency, transportation facilities, and industry.

Customs and Border Protection (CBP)

CBP continues to experience high numbers of incidents involving illicit use of unmanned aircraft systems to facilitate unlawful movement of people and narcotics across the Southwest Border. Transnational Criminal Organizations (TCOs) and possibly Foreign State Actors use UAS to conduct unauthorized surveillance of CBP personnel and operations to pass information to contacts on the ground on where to guide noncitizens or transport illegal drugs to circumvent law enforcement. Sensor records, pilot and agent sightings, and other sources of information also indicate the increasing use of drones to transport illegal drugs and other contraband across the border. This illicit activity threatens the safety of our front-line personnel, poses a collision risk to our aircraft, and adversely affects our border security operations.

Over a recent 5-month period, CBP sensors captured more than 30,500 drone flights within close proximity of the Southwest Border, of which 4,458 took place during nighttime hours. Additionally, more than 14,000 of these flights exceeded the FAA-regulated altitude of 400 feet, some nearly reaching altitudes of 4,000 feet. Among all these flights, there were only about 4,300 unique drone IDs, indicating that use of drones for illicit cross-border activity is not only wide-spread, but also organized and an integrated element of TCO operations.

The Act has enabled CBP to begin taking responsible C–UAS actions against systems that pose a credible threat to covered facilities or assets along the Southwest Border. Consistent with the Act and the DHS Secretary's Policy Guidance, CBP implemented a C–UAS policy and subsequent operations plan in July 2020 after extensive discussion and review to ensure lawful and efficient operational implementation. The overall volume of UAS traffic rapidly expanded in the past few years, and CBP is committed to identifying and targeting illicit activity while protecting lawful commercial and recreational use.

Currently, CBP operates C–UAS devices at select, high-risk locations along the Southwest Border. Operations target specific credible threats and do not involve persistent surveillance of all the border regions. Authorization for CBP C–UAS operations requires a credible threat determination that involves extensive analysis and evidence of the threat, including reports of visual observations and correlation with actionable information and other law enforcement information. All C–UAS operations adhere to authorized statutory and policy parameters to ensure operational integrity and compliance with all legal restrictions and privacy protections.

C–UAS operations are an essential capability to address evolving UAS threats and CBP implemented its risk-based C–UAS approach within a framework that ensures rigorous analysis and clear documentation of a credible threat to identify and target nefarious operators and devices amongst the increasing amount of drone traffic. Since CBP's implementation of C–UAS operations in July 2020, there were five credible UAS threats mitigated, affirmation of CBP's deliberate, targeted, and diligent application of its C–UAS authority.

C–UAS authorities will become even more critical as the UAS threat evolves. Less than a year ago, the Jalisco New Generation Cartel attacked Mexican law enforcement and a rival cartel with explosives deployed from drones. These incidents, along with indications that TCOs are pursuing the use of larger drones with more maneuverability, more payload capacity, and greater capability—to fly longer, higher, and further—are concerning trends. CBP needs these critical authorities to continue efforts to counter rapidly evolving threats and expand its risk-based implementation of C–UAS operations to additional locations along the Southwest and Northern Borders.

GAPS IN CURRENT DHS AUTHORITY

On December 21, 2021, DHS submitted the interagency coordinated and statutorily-required DHS C–UAS Assessment to evaluate drone threats to domestic critical infrastructure and airports, evaluate current Federal, State, local, territorial, or Tribal (SLTT) law enforcement authorities to counter drone threats, and identify additional improvements needed for security. The assessment notes the accelerated technological evolution of drone capabilities across a variety of commercial and recreational applications. As UAS capabilities advance, technologies to detect, identify, monitor, and track UAS must also advance.

The assessment also explains how current legal authorities do not expressly authorize DHS to conduct certain persistent UAS detection and mitigation activities, leaving our Nation's large hub airports and critical infrastructure vulnerable to intentional UAS threats and unintentional hazards. Additionally, the assessment identified gaps in existing authorities that limit the abilities of SLTT law enforcement to effectively deter unauthorized activities, respond to incidents, and enforce laws and regulations. Specific authority for protecting airports and transportation systems combined with a community-based approach to UAS detection would help set both the stage for improved air domain awareness and foundation for threat discrimination and mitigation efforts. These concerns are detailed in the Assessment.

DHS has been working closely with the administration and interagency partners on a legislative proposal to request reauthorization of our current C–UAS authorities. The Department's approach to reauthorization is grounded in its assessment of the evolving threat landscape as well as addressing key gaps and vulnerabilities that we have identified. We look forward to engaging with you, your staff, and other key stakeholders on those authorities.

CONCLUSION

DHS is committed to countering the threat of malicious UAS activity facing the homeland. We are grateful for the continued support of Congress and to our fellow departments and agencies for their support and contributions in this effort. Together we can raise the domestic UAS security baseline, disrupt attacks, and hold accountable those who perpetrate these acts. Thank you again for the opportunity to testify today and we look forward to your questions.

Chairman CORREA. Thank you very much, ma'am. I recognize Rear Admiral Clendenin to summarize his statement in 5 minutes as well. Welcome, sir.

STATEMENT OF SCOTT W. CLENDENIN, ASSISTANT COMMANDANT FOR RESPONSE POLICY, U.S. COAST GUARD, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral CLENDENIN. Good morning, sir. Chairwoman Coleman, Chairman Correa, Ranking Member Gimenez, Ranking Member Meijer, and distinguished Members of the subcommittee, thank you for the opportunity to discuss the Coast Guard's capabilities to counter the emerging threats posed by the malicious use of unmanned aircraft systems in the United States.

As the principal Federal agency responsible for the safety and security of U.S. ports, inland waterways, and along more than 95,000 miles of coastline, the Coast Guard works collaboratively with relevant stakeholders to combat threats in the Nation and maritime critical infrastructure and key resources. The novel threats posed by UASes are increasingly concerning as a proliferation of small UAS continues to increase in the maritime domain.

Over the last 4 years, the Coast Guard observed significant increases in UAS activity in the maritime domain as well as an acceleration in the rate of suspicious UAS sightings over or near maritime assets or facilities, such as ferries and cruise ship terminals and refineries. Over the same period, UAS interfered with or crashed into Coast Guard assets, ferries, cruise ships, and other

commercial vessels over 80 times. These numbers, which are concerning, only represent the events that were formally reported, verified, and analyzed.

UAS usage in the maritime domain requires additional risk consideration as a part of the operational planning cycle. This is important because there are no flight restrictions or commercial maritime critical infrastructure and key resources. And the owners and operators of those facilities have consistently expressed their concern about the threats posed to their facilities by UAS.

The Coast Guard views the ability for maritime critical infrastructure and key resources, facilities owners and operators to obtain flight restrictions as an important step in securing the airspace over the maritime environment, and is working with the Federal Aviation Administration to address these concerns. In addition, the Coast Guard coordinates all counter-UAS activities with the Federal Aviation Administration, the Department's Counter-UAS Program, and other relevant law enforcement stakeholders to ensure appropriate frequency and spectrum management protocols are followed to mitigate National airspace system impacts.

Since the enactment of the Preventing Emerging Threats Act the Coast Guard has conducted 26 separate counter-UAS events requiring Federal Aviation Administration coordination, including 5 special event assessment rating and 2 National special security events. Before deploying its counter-UAS capabilities for these types of events, the Coast Guard conducts a thorough review to ensure the appropriate protection of civil liberties and privacy rights for those individuals who could be impacted by counter-UAS operations.

The Coast Guard also closely collaborates with the Federal Aviation Administration for the generation and release of public notices advising UAS operators and the public of the location and time period when the Coast Guard will be conducting those operations. We take our responsibility to protect the maritime critical infrastructure and key resources and events with the maritime nexus seriously and we look forward to the renewal of the counter-UAS authorities granted by the Preventing Emerging Threats Act, which enabled counter-UAS operations in support of the Nation.

Thank you for your enduring support to the Coast Guard and your interest in this growing mission area. I look forward to your questions.

Chairman CORREA. Thank you very much for your testimony. I now recognize Mr. Gould to summarize his statement for 5 minutes.

STATEMENT OF AUSTIN GOULD, ACTING DEPUTY EXECUTIVE ASSISTANT ADMINISTRATOR FOR OPERATIONS SUPPORT, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. GOULD. Good morning, Chairman Correa, Chairwoman Watson Coleman, Ranking Member Meijer, Ranking Member Gimenez, and distinguished Members of the subcommittees. Thank you for the opportunity to discuss TSA's counter-unmanned aircraft systems, or C–UAS, activities.

From its creation in the aftermath of 9/11, TSA has dedicated itself to strengthening the security of our Nation's transportation systems while ensuring the freedom of movement of people and commerce. Unmanned aircraft systems represent a recent challenge to this security.

As you may recall, in December 2018, London's Gatwick Airport was shut down for 33 hours following drone sightings over the airport. This was a wake-up call for the aviation sector. The result of the shutdown was the cancellation or delay of over 1,000 flights, disrupted travel plans for around 140,000 passengers, and economic losses estimated in the tens of millions of dollars.

The United States has also seen instances where aviation operations were disrupted by drones. In January 2019, 1 month after the Gatwick incident, Newark Liberty International Airport in New Jersey was closed for over an hour after a drone sighting. In March 2021, the Greensboro/High Point Airport in North Carolina closed for 2½ hours due to drone sightings.

TSA has seen a steady increase in UAS events reported near transportation systems. For calendar year 2021, nearly 2,000 UAS events were reported to TSA. This was a 110 percent increase over the previous year. Of those events, about 1,500 occurred near airports, including 686 near major or Core 30 airports. While most of these events did not impact air operations, I want to highlight that since the beginning of 2021, 49 of these events required an aircraft to take evasive action and 5 of these were commercial flights.

In October 2018, Congress passed the Preventing Emerging Threats Act, providing DHS and DOJ the authority to use counter-UAS systems to protect certain covered facilities and assets as determined by the Secretary and the Attorney General. While TSA was not provided specific authority in the act, the law provides limited authority for DHS to carry out activities related to the protection of an active Federal law enforcement investigation, emergency response, or security function that is limited to a specific time frame and location. To that end, response to a persistent drone at an airport constitutes such an emergency response.

After the Gatwick event, Federal agencies, including the Department of Justice, Department of Defense, Federal Aviation Administration, and the Department of Homeland Security drafted a Concept of Operations outlining how the Federal Government would carry out actions to mitigate a similar event at one of the Core 30 U.S. airports. This CONOPS designated TSA as the lead Federal agency for such a response. Any use of TSA's authority for response to a threat would include Secretary approval and close coordination with the Federal Aviation Administration.

Since the passage of the act and signature of the CONOPS, TSA is prepared to protect airports and threats posed by UAS. TSA maintains a team of Federal air marshals to execute DHS-authorized UAS response at covered facilities or assets. TSA also uses this team to conduct UAS-specific joint vulnerability assessments, or JVAs. Since February 2021, TSA has conducted these JVAs at 17 of the Core 30 airports and will complete the remaining by the end of 2022.

TSA also requires the Federal security director, or FSD, at every airport to develop a tactical response plan which outlines roles and

responsibilities during a UAS event. Federal security directors conduct annual tabletop exercises of these plans with local stakeholders, including airport authorities, local law enforcement, the Federal Aviation Administration, and other Federal agencies.

Last, to support the development of C–UAS capability in airports TSA has established a technology test bed at the Miami International Airport where TSA, in coordination with DHS S&T and the Federal Aviation Administration, evaluates, detect, track, and identify technology, including radar, thermal imaging, and electro-optical cameras. These tests do not currently involve counter or mitigating capability and are intended to assess the performance of tracking technology in an airport and ensure that technology complies with DHS outlined privacy measures. The results will help us understand which technologies are effective in actual airport environments.

Thanks to your support TSA has the funding it needs to establish a second test bed at Los Angeles International Airport, one of the top airports for reported sightings. This funding will help us determine what equipment is best suited to identify threats.

I appreciate the committee's interest in this important issue. I look forward to answering your questions. Thank you.

Chairman CORREA. Thank you, sir. Now I recognize Mr. Michelini to summarize his statement for 5 minutes. Welcome, sir.

STATEMENT OF DENNIS J. MICHELINI, DEPUTY EXECUTIVE ASSISTANT COMMISSIONER FOR AIR & MARINE OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. MICHELINI. Thank you, sir. Good morning, Chairs Correa, Watson Coleman, and Ranking Members Gimenez and Meijer. It is an honor to be here today on behalf of the U.S. Customs and Border Protection to discuss CBP's counter-UAS operations.

I started my career in border security more than 27 years ago, first with the U.S. Border Patrol and then transitioning to Air and Marine Operations. Nearly 10 years of my law enforcement career have been dedicated to UAS activities and I have witnessed firsthand the evolution of the UAS threat at our borders.

There are three areas I would like to highlight: The current threat of UASes at and near the border; how the critical authorities granted by the Preventing Emerging Threats Act enables us to respond; and the importance of improving domain awareness to identify, deconflict, and mitigate credible threats.

Transnational criminal organizations use drones to conduct unauthorized surveillance of law enforcement personnel and their activities. This results in organized criminals on the ground becoming acutely aware of law enforcement's location. With that information criminals and smugglers are then able to evade detection by law enforcement and facilitate the unlawful movement of people and illegal drugs into the country.

Additionally, drones transport goods. Although they have limited payload capacities, the potential risk is significant. For example, a hobby drone can manage about 4½ pounds of payload. If that 4½ pounds was strictly fentanyl with a 10 percent purity, that single

drone would be transporting 80,000 legal doses into the United States. That is one drone.

The overall volume of UAS traffic, both for legitimate recreational and commercial purposes and criminal intent, has rapidly expanded in the past few years. Over a recent 5-month period, CBP sensors captured more than 30,000 drone flights within close proximity of the Southwest Border. Nearly 15 percent of those occurred at night, which is in violation of FAA daytime operational regulations, and nearly half exceeded the FAA regulated altitude of 400 feet, some reaching altitudes of 4,000 feet. However, among these more than 30,000 flights, there were only about 4,300 unique drone IDs, indicating repeat violations by the same UAS operators.

This illicit use of UAS threatens the safety of CBP's front-line personnel, poses a risk to our aircraft, and adversely affects our border security operations. However, thanks to Congress' passage of the Preventing Emerging Threats Act, CBP has been enabled to take targeted and deliberate counter-UAS actions.

Consistent with the act and DHS policy, CBP implemented a counter-UAS policy and subsequent operation plans in July 2020 to ensure efficient and appropriate application of this authority. As authorized by DHS Secretary, CBP operates counter-UAS devices at select active locations on the Southwest Border and targets specific threats to covered facilities or assets while ensuring the protection of civil rights and civil liberties.

Authorization for counter-UAS operations is a methodical and thoughtful process. It requires a credible threat determination based on extensive analysis and evidence.

Since CBP's implementation of the counter-UAS operations there have been a number of credible UAS threats mitigated. As operations expand we will continue to apply our counter-UAS authority with the same prudent and targeted application to effectively identify nefarious operators and devices amongst the expansive amount of legitimate drone traffic.

As technology evolves, counter-UAS authorities will become even more critical. We have seen evidence of TCOs pursuing the use of larger drones with more maneuverability, more payload capacity, and greater capability to fly longer, higher, and further. This means that we will require a continued commitment to achieving persistent domain awareness.

Having the ability to fully understand the environment in which a threat is operating is critical to protecting lives and countering criminal organizations. With your continued support CBP will further efforts to counter this rapidly-evolving threat and expand our risk-based, data-driven implementation of counter-UAS operations.

I thank you for the opportunity to appear today and look forward to your questions.

Chairman CORREA. Thank you, sir, for your statement. I want to thank all the witnesses today. I will remind the subcommittee that we will each have 5 minutes to question the panel and I will recognize myself for 5 minutes of questions.

I will start out by, Mr. Michelini, if I may, I was disturbed by your statement because it shows the emerging threat of these drones in many ways. That is the defense side. What about the offensive side? Are you looking at using—are we using drones at the

Northern and Southern Border to make sure that we are looking, observing those things that are going on at our borders?

Mr. MICHELINI. Absolutely. Small UAS and drones, both rather large up at altitude, or small UAS as deployed by both USBP and OFO, are used extensively. But in the context of counter-UAS it is that environment where you can understand who is the players on each side. That gets very, very complicated without the sophistication of a domain awareness technology out there.

But to go back to your opening statement, absolutely, both law enforcement and, of course, the cartels are using small UAS for their benefit.

Chairman CORREA. So, if I may ask, clearly when we develop policy we coordinate with Federal, local, State agencies to make sure that we are all on the same page. Do we do that also dealing with the Canadian authorities or the Mexican authorities and other nations that we may have to coordinate when it comes to drone activity?

Mr. MICHELINI. We absolutely do. Within the United States we coordinate, of course, with the FAA and State and local for any kind of work we are doing along the Southwest Border. There is a lot of coordination that has to get done between manned and unmanned, these small UASes, in the environment of the Southwest Border on the U.S. side. When dealing with, for instance, Mexico, there are resource restraints on either side, and so while we can be mitigating threats from small UASes crossing the border back and forth, and through further investigations, both us and the Mexican law enforcement can work together.

But I would have to say is on a case-by-case basis with just——

Chairman CORREA. When you say you can work together, what do you need to actually work together between consistently?

Mr. MICHELINI. Well, yes, at the ground level the relationships are fantastic, again, with resources available. There is a lot of moving parts on the Southwest Border.

On the northern side, for the detection that we employ, that is done by just us on the U.S. side. That is I am not aware of any mitigation capabilities or domain awareness for small UAS on the southern side.

Chairman CORREA. Mr. Michelini, my questions are really directed at trying to anticipate this area that is already a very threatening emerging challenge. We would love to, as policy makers, get ahead of it, so that as we move forward we were there instead of what we should have, could have. Let us get ahead of this threat.

Second of all, let me move in my last 2 minutes to Ms. Vinograd. To what extent has the Department of Homeland Security included the Office of Civil Rights and Civil Liberties and Privacy Office in developing your guidelines and policies?

Ms. VINOGRAD. Chairman, thank you for such an important question. As I mentioned, the Department's C–UAS mission is to mitigate credible threats to the safety and security of DHS missions and to do so in a way that is consistent with privacy and civil rights and civil liberties. DHS conducts every single C–UAS operation consistent with the privacy provisions and civil rights and

civil liberty provisions in the act as well as the First and Fourth Amendment and other relevant Federal statutes.

The Department does have DHS-wide policy guidance that has a specific annex on privacy and civil rights and civil liberties, developed in close coordination with our chief privacy officer and civil rights and civil liberties officer. Further, every component that engages in C–UAS operations has component-specific privacy and civil rights and civil liberties guidance. Every authorized individual within the Department that engages in C–UAS operations is required to receive training specifically on the act and the existing privacy and civil rights and civil liberties provisions.

Finally, sir, the Department has published a public privacy impact assessment. Every component program, in coordination with our privacy officer, every component program must be accompanied by a privacy threshold assessment and, where needed, a specific privacy impact assessment.

Chairman CORREA. Thank you very much for your comments. It seems that I am out of time. I will now recognize the Ranking Member of the committee, Mr. Meijer, for 5 minutes of questions.

Mr. MEIJER. Thank you, Mr. Chairman. I want to get a little bit more into the authorities, Mr. Michelini. Since CBP started using the authorities in the act in late 2021, you mentioned several of the UAS incidents had been mitigated and the drug seizures that have resulted and the arrests that have followed from those. How is CBP looking at continued use of the authorities and what is the alternative if there is an expiration of these authorities in October?

Mr. MICHELINI. Well, the authorities are essential for both domain awareness, seeing the threat environment, and mitigating the nonparticipant actors that you want to. It would be very hard to go forward in an environment where the authorities ere not established. It is—I am sorry, sir.

Mr. MEIJER. Please.

Mr. MICHELINI. It is a tidal change what is happening with small UAS strategically on the interplay between what is going on on the Southwest Border. I think you are going to hear it from any of the members here today and the panelists, the change is—we have had 5 near misses with small UAS in the last year and a half. In an environment, in a helicopter like I used to fly where there is not supposed to be a lot of players around, that is pretty staggering. We have had just in the last year-and-a-half thousands of crossers of small UAS. It is a subject that has to get addressed and I believe the Department is doing an excellent job of moving forward in a thorough and methodical fashion to get this done.

Mr. MEIJER. Rear Admiral Clendenin, kind-of a similar question on your side. You know, obviously, CBP, there is a little bit more flexibility when we are talking about an international border and some of the restrictions and implicit authorities there. But within kind-of Coast Guard's broader domain or just homeland security in general, what is your view on how—what restrictions would we put in place or what opportunities that we currently have to protect the homeland, to protect against, you know, counter-UAS if these authorities were to expire in October?

Admiral CLENDENIN. Ranking Member, in short, we would not be able to conduct these operations without the provisions of the Pre-

venting Emerging Threats Act. Right now the provisions are sufficient for our operations as we run them, but we also share the concern of the proliferation of the use of UAS around secure facilities and assets. So we would look forward to the continuation of the PETA act, sir.

Mr. MEIJER. Thank you. Shifting a little bit to Mr. Gould, can you explain TSA's role in protecting against UAS around commercial airports? I know you mentioned kind-of those top 30 airports, but does TSA need additional authority to be able to successfully protect, you know, a broader array of airports? I represent Grand Rapids, Michigan, and we are not a top 30 airport, you know, we are top 100. What does the expansion of that counter-UAS capability look like? As I mentioned, is there additional authorities needed to protect a broader array of civil aviation assets?

Mr. GOULD. Yes, sir. Thank you very much for that question. The authority we have right now allows us to, as you said, conduct counter-UAS operations in Core 30 airports subject to the approval of the Secretary. That omits airports like you mentioned, your home airport.

Right now we are involved in doing joint vulnerability assessments of these larger airports, which identify drone launching sites, potential areas for surveillance where a drone operator can cause an issue at an airport. We also do our tactical response plans and our exercises annually. We are radically advancing our knowledge of UAS activity around airports through our test bed in Miami.

However, our ability to respond is purely reactive at this point. I believe that authorities that would allow us to be more proactive, particularly in terms to detect, track, and identify, to assess when there is a threat, where it is coming from, and respond accordingly will be essential moving forward. Thank you.

Mr. MEIJER. Thank you. No, and I think, you know, obviously we are looking at both the accidental and the intentional use of UAS to cause harm. You know, Mr. Michelini, as you mentioned, you wouldn't expect border airspace at lower altitudes to be congested, but when you have rotary wing assets that are going through and potentially running into these, you know, it is only a matter of time before we lose the alliance of some of our brave folks who are guarding down there.

With that, Mr. Chairman, I yield back.

Chairman CORREA. Thank you very much. I now recognize Chairwoman Watson Coleman for 5 minutes of questions.

Chairwoman WATSON COLEMAN. Thank you very much, Mr. Chairman, and thank you to the witnesses for sharing your information. I want to start with a question to Secretary Vinograd. How frequently or regularly does DHS interact with and collaborate with the civil rights and civil liberties entities that expressed concern about this bill and this authority?

Ms. VINOGRAD. Chairwoman, thank you. The Department of Homeland Security is working through the Office—our chief privacy officer and the Office of Privacy as well as our Office of Civil Rights and Civil Liberties does engage with members of the communities that you have mentioned.

Further, as we look forward and as we acknowledge the escalating threat environment as well as the need to judiciously apply any authorities that DHS currently has or may be granted going forward, DHS is committed to continuing engagement with members of the communities that you described to ensure that we understand the concerns.

Chairwoman WATSON COLEMAN. Thank you, Assistant Secretary. I want to get a handle on understanding how regularly you interact, get feedback from, and give information to these organizations and entities because they have serious concerns. I get it that drones can be really a real threat, those that are intentionally malicious and those that are innocent. But what I want to know is, how—to what degree are we respecting those concerns of those agencies or entities? So, how regularly does your Department, whatever office it is, interact with them?

Ms. VINOGRAD. Chairwoman——

Chairwoman WATSON COLEMAN. If at all.

Ms. VINOGRAD. Chairwoman, thank you. I can tell you today that we regularly interact with members of those communities. I am happy to follow up with you after this hearing with more specific information and details on those interactions.

I will say this——

Chairwoman WATSON COLEMAN. Thank you.

Ms. VINOGRAD [continuing]. The C–UAS program at DHS is not a surveillance program. It is used to mitigate credible threats. The C–UAS program is also deeply focused on transparency.

Chairwoman WATSON COLEMAN. I am there with you. I am there with you. I really appreciate your willingness to get to me after the fact. I specifically would like to know what DHS's policy is and actually what it has done as it relates to consistent, dependable interaction and collaboration with these groups. So, through the Chairman of this subcommittee meeting, I would like to ask that information be sent to us.

Again, I would like to ask you what data precisely is captured during a UAS mitigation? Do you believe DHS could under the current statute capture additional data or are there existing statutory protections against capturing more data than is strictly necessary to mitigate the UAS?

Ms. VINOGRAD. Chairwoman, thank you. Under the provisions of the act DHS currently only collects data on the signal between the control device and the UAV. That includes, for example, telemetry and location information. Currently, the Department of Homeland Security does not collect and is not able to access, for example, call logs or text messages or the contents, let us say, of what the control device actually is.

Further, consistent with the act, DHS only retains that data for under 180 days. Again, it is not the intent of any C–UAS operations to collect any personal information that may be related to the control device or the UAV. DHS has judiciously respected these provisions in the act and will continue to do so going forward.

Chairwoman WATSON COLEMAN. Listen, I did have another question, but I really don't have enough time, so let me just share this. I am someone that believes that drones are a potential threat, that they are a real threat, and that we do need to have protection of

our safety and security. I also believe very, very intently that our values are mightily important to protect as well, and that is our privacy, our due process, and things of that nature.

So, I am very much interested at some point in just hearing what you think is missing, what you think you all need more of, how you respond to some of the areas that we think there needs to be a clarity in understanding exactly what you can engage in and how you can engage in and how you can act when you issue warrants, et cetera.

With that, Mr. Chairman, I am going to yield, but there are so many more questions that we do have with regard to the implementation, the appropriate implementation, of legislation of this nature. I yield back.

Chairman CORREA. Mrs. Watson Coleman, I couldn't agree with you more. So many more questions. Thank you very much for those.

I would like to recognize now the Ranking Member of the Subcommittee on Transportation and Maritime Security, the gentleman from Florida, Mr. Gimenez, for 5 minutes of questions. Welcome, sir.

Mr. GIMENEZ. Thank you, Chairman Correa. I also couldn't agree more with Chairwoman Watson Coleman about not only is it a threat, the coming threat, we have a threat now, but I think it is actually going to get worse. So I have a series of questions.

First, I want to relay something that happened to me in like around 2017. I had the privilege of going to Israel as the mayor of Miami-Dade to look at technology. I can tell you that the Israelis were extremely concerned about drones, especially around the airport, Ben Gurion Airport. That is why really at MIA we have a pilot program right now because of that concern that came out of that trip to Israel.

There are two concerns that I have. The current technology is piloted unmanned air systems, but I am actually more concerned about future technology, or maybe current technology, which is unpiloted unmanned aircraft systems, basically a system where you can actually tell it what to do and it goes off. Right now we have lot of capability in intercepting and interfering with communications with piloted, you know, unmanned air systems. I don't believe we have any capability about unpiloted because they are not being piloted by anybody. They are basically intelligent.

Going back, though, to the border, Mr. Michelini, you see thousands of unmanned air systems flying around all the time at the Southern Border. You see them, you detect them, you know what they're doing and all that. What can you do about them?

Mr. MICHELINI. The commanded and non-commanded, those are complicated subjects that I think in a—there are some options out there, but I think we should maybe talk about that in a closed hearing for that.

Mr. GIMENEZ. Fair enough.

Mr. MICHELINI. But for the piloted one, it is not just what you see, it is the preponderance of what you don't see. I had a story I can remember hearing like a year-and-a-half ago is one of the first times we put—we turned on these devices, they saw 40 or 45—and by the way, these are not—the ranges of what they see are

not very far. They saw 40 targets that nobody was aware of. Both counter drone on the—it was counter, counter for the—on the Mexican side, and also, small UASs crossing the border. So, the amount out there is really staggering. This authorization, though, is the foundation to how we are going to address our domain awareness gaps on the Southwest Border. It is essential to keep this running.

Mr. GIMENEZ. Do you have the authority to take them down if they are considered to be a threat?

Mr. MICHELINI. We do mitigate. We do mitigate small UAS. It is a methodical process. We set up an area that we have a high risk and we walk through a process that is built to trickle down from the DHS policy straight to CBP. So, we do have that authority.

Mr. GIMENEZ. Now, Mr. Gould, I still have a concern, a major concern of we can see them, we can interrupt them, interrupt their capabilities once they get into a—there is a zone, right? There is a barrier. There is like a fence, right? Those piloted unmanned aerial systems we could do something about, or many of them. It is the unpiloted aerial systems that really concern me and the capabilities that they may have in the future, especially carrying destructive payloads, OK, into an airport. Do you have the authority now to take these down if they cross over into restricted air space?

Mr. GOULD. Sir, DHS has the authority to mitigate counter-UAS in accordance with an emergency response or a security incident like I discussed in my opening statement. As a lead Federal agency, TSA is—TSA is the lead Federal agency under that authority. In terms of having the capability to actually do that today, we do not.

Mr. GIMENEZ. Fair enough.

Mr. GOULD. We are focused on detect, track, and identify. I would like to highlight your concern. I met with the Center for the Protection of National Infrastructure, which is the United Kingdom's version of infrastructure protection, prior to this hearing to discuss the Gatwick incident. They believe that at least on some of those flights, when Gatwick shut down it was a drone operating exactly as you said. No connection to a ground control station, purely by GPS waypoints. Difficult to detect, difficult to interdict.

Mr. GIMENEZ. Thank you. Mr. Chairman, I think that we need to probe further into this about what we are doing about are we funding sufficient research in order to obtain offensive capability, a defensive capability which is offensive in nature, we are basically taking them down. Because I really do believe that it is a matter of when, not if, some—a major event is going to be happening either at the border, or is going to be happening at one of our airports, or one of our transportation hubs through the use of these unmanned systems. Thank you, and I yield back.

Chairman CORREA. Mr. Gimenez, I couldn't agree with you more. What I would like to do is follow up with a closed discussion with Mr. Michelini on some of these issues at the border and these drones. So, I would like to have the staff try to schedule that. Thank you very much. Now, I would like to recognize Mr. Payne for 5 minutes of questions. Welcome, sir.

Mr. PAYNE. Thank you, Mr. Chairman.

Chairman CORREA. Welcome.

Mr. PAYNE. Thank you, sir. Mr. Gould, several unmanned aircraft systems incursions have been reported at airports and the one you mentioned at Newark Liberty International in January 2019, where planes were altered and diverted for over an hour as you stated. Would you briefly discus the ability of drones to disrupt airport operations and what impact this has on travelers and airport employees. Are there measures Congress can take to support Transportation Security Administration to address this threat?

Mr. GOULD. Thank you very much for the question, sir. With respect to the incident, New York Liberty—or New Jersey—Newark Liberty International Airport, the drone actually was not that close to Newark. It was flying at 35,000 feet over Teterboro Airport, which is a municipal airport sort-of adjacent to Newark.

Mr. PAYNE. Yes.

Mr. GOULD. But it was in a flight path for Newark International Airport. Thirty-five hundred feet is far above the altitude that a drone operator is allowed to fly. They are limited to 400 feet. It was high enough to interfere with a flight path. That interference at an airport is—has an exceptional, exceptional effect. Flights need to be diverted. They need to be rerouted. Airports sometimes are large enough where you can just use a different runway. However, the drones are mobile. If it was someone who was determined to really cause a disruption to the air space, they could just relocate the drone to the new air space that is being used.

So, it is a significant problem with a cascading effect of airport delays, inconvenience to travelers, disruption of airport workers, disruption of security. It is a very, very significant event.

Sir, I am not sure if you had more than that that you asked. I couldn't quite hear the end of your question.

Mr. PAYNE. I asked what could Congress do to help you along the way in addressing, you know, to support the TSA in addressing the threat?

Mr. GOULD. Sir, thank you very much for that. I think, like the other witnesses, I think renewal of this authorization is essential. From TSA's perspective, not only to Mr. Meier's question earlier about would we go beyond the core 30 airports, which increased authorities would allow us to do, it would also allow us to protect other modes of transportation because this is not unique to the airport environment. Pipelines, refineries, railroads are all subject to unmanned aerial systems incursions that right now we do not any authority to respond to. Thank you.

Mr. PAYNE. OK. Thank you. Mr. Chairman, in light of the size of the committee today, I will yield back.

Chairman CORREA. Thank you, Mr. Payne. Now, I recognize Mr. Bishop for 5 minutes of questions. Welcome, sir.

Mr. BISHOP. Thank you, Chairman Correa. Mr. Michelini, as I am listening and I understand there is this authority needs to be renewed. I don't know the details in the confines of the authority, but what I think I heard you say or it comes out in the testimony in the memos I have looked at, is there is a lot of—there are a lot of drones flying back and forth across the U.S.-Mexico border. Is that correct?

Mr. MICHELINI. That is correct.

Mr. BISHOP. I don't think your microphone came on. But that is correct.

Mr. MICHELINI. Correct.

Mr. BISHOP. OK. You gave a couple figures. I don't know whether they include both things that are drones just on the U.S. side and those going back and forth, but you mentioned 4,300 unique IDs. In other words, 4,300 different drones up in the air and 30,000 flights in the last 6 months. Is that what you said?

Mr. MICHELINI. That were recorded, correct.

Mr. BISHOP. That you recorded. You know, so, anyway we get new terms, you know. We got UAS and then we got C–UAS, counter-USOs, I would say anti-drone mechanisms, that you got available. Sounds like they are surveillance things so you can pick out more of them. Is that right? You can find them. You can see them.

Mr. MICHELINI. So, with the counter-UAS technology we have, it—I want you to think of it as both, you know, to detect and mitigate. Typical radar that is used in the manned aviation environment, they are not really picking this up. So, when we started down this process of counter-UAS, it was both the technologies to detect and then the technologies with the authorities to mitigate.

Mr. BISHOP. So, mitigate, if I read the memo or it was maybe a summary of the memo correctly, it sounds like you can maybe jam a transmitter and force the thing to land or something. Is that sort-of the right idea?

Mr. MICHELINI. Right. There is communication between—not to go down that other line—but there is communication between the operator and the small UAS or drone. When the communication is just interrupted, usually what happens is, whether you own a small UAS or not, it will have a return to home or some sort of land function to it.

Mr. BISHOP. OK. So, I get it. I get mitigation sounds pretty timid and so does that when I hear it described. I mean, Mr. Gimenez asked a question, do you have the authority to take them down? I can't understand. Maybe you could just help me understand. Are there legitimate reasons for cross-border drone flights? Because we don't allow anybody—I mean, well, we are not supposed to allow anybody to come into the United States. Unfortunately, in the current state of affairs, we allow tons of people to come into the United States illegally. But I don't understand the reason that we would allow drones to come into the United States. Why don't we shoot them down?

Mr. MICHELINI. Well, in a kinetic response like that, we don't—we haven't—CBP is mitigating by bringing them out of the sky. They are returning to the ground, but we have not done kinetic responses like that.

Mr. BISHOP. Yes, I guess I am asking as a policy matter if you are able to speak to it. Maybe not, I will get Ms. Vinograd, but—if that is the right pronunciation of your name. Forgive me, I didn't catch that earlier. But what is the policy reason? I am just thinking about it from the perspective of Americans watching this hearing that may say, well, why would we allow? Staff had a notation in the memo that one drone has had 1,500 flights across the border. I don't understand why we permit that.

Mr. MICHELINI. Well, it is not for not trying, sir. This is a brand-new technology that we are forwarding to the Southwest Border. What we look for are specific areas that there is a high risk, multiple crossers, and then we set up with what technology we have, and we begin a, you know, a con op, an operation in that location. But it has, like I said, there is a lot going on right now that this Act is helping us finally target and address.

Mr. BISHOP. I hear you. I am concerned about whether the Act goes far enough, I guess, is what I am trying to ask about.

Mr. MICHELINI. Understood.

Mr. BISHOP. So, I get that you said that the drones are used by Mexican cartels, both to detect your movements and locations so that they can facilitate smuggling with it. I think you said they are flying in drugs. We know what a small quantity of fentanyl will do.

Mr. MICHELINI. Mm-hmm.

Mr. BISHOP. So, they can fly drugs into the United States.

Mr. MICHELINI. Yes, in small amounts. But again, just the idea of being overhead to help move a group that might be backpackers with drugs, which could be even more, is a fantastic strategic tool by the cartels. So, both are very nefarious and very dangerous.

Mr. BISHOP. Yes. Yes, how do I pronounce your name?

Ms. VINOGRAD. My last name is Vinograd.

Mr. BISHOP. Vinograd.

Ms. VINOGRAD. Indeed.

Mr. BISHOP. I beg your pardon. Ms. Vinograd, you are the policy person here.

Ms. VINOGRAD. Yes.

Mr. BISHOP. Why are we content to let Mexican cartels operate drones to cross the United States border? Why don't we take them down? Why isn't that a threat to the United States National security? We wouldn't allow airplanes to fly in, would we?

Ms. VINOGRAD. We would not. Let me assure you, sir, that the Department does not believe that it is appropriate or acceptable for cartels or transnational criminal organizations, more generally, to bring illicit substances across the border. Currently, the Secretary has designated parts of the Southwest Border as a covered facility or asset, which gives my CBP colleagues the authority to track—excuse me—to detect, identify, track, and mitigate C–UAS that pose a credible threat to DHS mission sets.

At this juncture, CBP, and I will defer to my CBP colleague, feels confident that they have the appropriate authorities as well as operational plan to mitigate these threats. We are consistently reviewing the threat environment, both as it pertains to what parts of the border are designated as covered facilities or assets, and whether additional mitigation technologies are needed. In a closed hearing, sir, we would be glad to go into further details on what those mitigation techniques look like.

Mr. BISHOP. My time has expired, Mr. Chairman.

Chairman CORREA. Thank you. I just wanted to follow up on your comments, which is I would love to, in a closed hearing, talk to Ms. Vinograd and Mr. Michelini about how many of those are actually real threats? How many of those are just people, knuckleheads, who don't understand that this toy is actually caus-

ing possible dangers to themselves and other people and other assets?

You know, you go down to the local store, you buy one of these drones. You decide to fly it up. I just I am wondering if this is an educational issue where people don't understand this is not a toy in the context of its use. Anyway, we will talk about that in a closed session later on.

Now, I would like to recognize Ms. Titus from Nevada for 5 minutes of questions.

Ms. TITUS. Well, thank you, Mr. Chairman. Just going back to Mr. Bishop's point about why don't we shoot them down? I don't think it is quite that simple. I don't think you start firing off rockets to shoot down drones in neighborhoods or along the border or along the river where people live and all. Could maybe Mr. Gould just address that? Some of the problems that would exist if we just start firing off rockets to shoot down these drones.

Mr. GOULD. Well, thank you for the question, ma'am. Right now, from a TSA perspective, we are focused solely on detect, track, and identify in the airport environment. Airports have a lot of ambient energy. Detection systems that might work in a very open area will be adversely affected by that ambient energy. Our ability to mitigate a drone event at an airport really is predicated on our ability to find it and ensure that it has some sort of nefarious intent or inadvertent encroachment on an air space.

With respect to mitigation, like I said from a TSA perspective, we are not quite there yet. We do consider the communications link disruption that will bring the drone down to a safe landing either by the operator or in a predetermined location. In terms of actual kinetic responses like had been discussed, we are not really contemplating that yet.

Ms. TITUS. Well, and just to continue that conversation. I know that in Las Vegas a lot of people are using drones within that 5-mile parameter around McCarran Airport to try to take pictures of the Las Vegas Strip, which is right at the heart of my district. You know, they know they are not supposed to be there. I don't know if you consider taking pictures of the Strip nefarious or not, but certainly, they cause harm. Often they make a plane have to be diverted or can't take off or something like that. Could you talk a little bit more about what we could do as Members of Congress to help you deal with those kinds of threats?

Mr. GOULD. Well, right now, thank you very much to the Congress for funding our test bed——

Ms. TITUS. I am sorry, I can't hear you.

Mr. GOULD [continuing]. In Miami and soon to be Los Angles so we can do detect, track, and identify activities.

Ms. TITUS. Hello? I lost you. Reed? I lost him.

Mr. GOULD. Ma'am, are you there?

Ms. TITUS. Reed?

Chairman CORREA. Hello?

Ms. TITUS. I am sorry, Mr. Chairman. I can't—they just turned off.

Chairman CORREA. We are here. Can you hear us?

Ms. TITUS. I can't hear them.

Chairman CORREA. Ms. Titus, can you hear us? Hello?

Ms. TITUS. I didn't touch anything.

Chairman CORREA. A drone attack. Can you answer the question, if you can.

Mr. GOULD. Would you like me to finish the response?

Chairman CORREA. Yes, please.

Mr. GOULD. Thank you very much, Mr. Chairman. I am well aware of the drone situation in Las Vegas as well. The Las Vegas Strip is a very attractive location for people to film. There was a commercial aviation aircraft on final approach to Las Vegas that was actually tailed by a drone, photographing it not too, too long ago.

So, back to our detect, track, and identify mission that we are testing out in Miami, I cannot emphasize the importance of that work enough. It allows us to quantify the problem in the airport environment and to expand it to other airports. In Miami, specifically, we had about 105 reports of UAS in the last year from a visual reporting perspective using technology down there that never exceeds 20,000. Now, these are not all near the airport. It is in the greater Miami area. But many of them are clustered around the airport. Pursuing our detect, track, and identify capability will help us address that problem. Thank you, ma'am.

Ms. TITUS. Thank you. Well, Mr. Chairman, maybe we can work on some of that, it could be helpful to address this problem with TSA.

Chairman CORREA. Ms. Titus, you have a minute left.

Ms. TITUS. That is all right. I will yield back. That was mainly what I was concerned about. Thank you.

Chairman CORREA. Thank you, Ms. Titus. Now, I would like to recognize the gentlelady from Mrs. Harshbarger—the gentlelady from Tennessee, Mrs. Harshbarger. Ma'am.

Mrs. HARSHBARGER. Thank you, Mr. Chairman. I am a gentlelady. Thank you to the witnesses today. I do have some concerns and I would like to direct question to Mr. Michelini. You know, it was—you mentioned that these drones go from 400 foot to 4,000 and, you know, it is the same offenders time after time. There are going to be larger drones used to increase the payload that they are carrying.

You know, I have read reports that the drug cartels are using these drones to facilitate the movement of drugs, illegal drugs over the Southwest Border.

I guess my question is, I know Mr. Gimenez was talking about taking these drones out, but from what I understand, you can render the software useless and you can cut those off. I am looking at a recent report about a U.S. provider, Vector Graphics, editing software who closed access to the services for those drones. Is that a possibility? Do you know the make and model and what type? You have listed that there has been 4,300 drones identified because you do have to register those. But, you know, my question is what capabilities does CBP have to counter these transcriminal—transnational criminal and drug trafficking organizations on the border? Can we do that with that software?

Mr. MICHELINI. We absolutely can. I mean, for the hardware and software that we utilize across the Southwest Border, we can—we use other metrics necessarily than just their ID number. It is a lit-

tle complicated in that we are working very close with the FAA and that is how we deconflict what may be a rancher or somebody flying their small UAS and a nefarious character using a small UAS. It is not quite as easy as to do with a manned aircraft where it is on a radar target and you can see it. First you have to set up these counter-UAS devices and detect it.

One of the problems, though, is you could buy a small UAS right now and it might have a ceiling. It might have a built-in ceiling of 400 feet. If you take it out and try to fly it, the software knows where it is. Well, when you hear these examples about them flying higher, either that was pre-software or people have gone around the software kind-of limits on their platforms. So, while you can, you know, this is just how crime works is while you can set software limits in a piece of machinery, once you buy it, though, things can be altered.

Mrs. HARSHBARGER. Yes. Well, that is crazy. You know, 4,000 foot that is—that is BFR for a small aircraft, you know, a personal aircraft, personal pilot. So, you know, that is a little bit crazy. Do you know the models or which drones, I guess, you are confiscating more of? That is why I am asking. Or the make and model——

Mr. MICHELINI. We do know——

Mrs. HARSHBARGER [continuing]. Of those drones? Because, you know, DJI is a Chinese drone. I am just questioning what you are seeing.

Mr. MICHELINI. Well, they command about 80 percent of the market. So, predominantly, we would see that company. I don't have on me right now the specifics of the companies that we are tracking or the few that we have interdicted but that is information I could get to you.

Mrs. HARSHBARGER. Yes, that would be great. You know, and like you say, they can alter that software later on. It is terrible but we see the increase of drugs and the increase in the payload that they, you know, drop across the border is we already have problems. So, that is just going—it is not going to mitigate it all. It is just going to increase the problem with the drug flow. So, with that, Chairman, I thank you for your time and I yield back.

Chairman CORREA. Thank you, ma'am. Now, I would like to recognize the gentlelady from Texas, Ms. Jackson Lee, for 5 minutes of questions.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman, and Ranking Members of the respective Transportation and Oversight Committee. This is a continuous important issue and an issue that we should certainly focus on. Again, to the witnesses, let me express my appreciation.

Let me just simply say this is really about saving lives. I guess I immediately think of, in addition to the other elements of this problem, is loss of life in a flying commercial airline. Let me ask Rear Admiral Clendenin, if I would, and Mr. Gould, what is it most of all that DHS or the Department would like to do in the future to be more protective or to really to cease or to bring down the potential damage with the use of drones by individuals and possibly terrorists?

Admiral CLENDENIN. Thank you, Congresswoman. So, right now, we have the authorities and the capabilities we need to complete

our pilot program. Once we complete our pilot program, we will move to what we call program of record, a more permanent both in the types of systems we acquire and the numbers that we need to support our maritime security operations. As we do that, we will communicate with the Department and with the administration and with Congress for any additional needs. But as we stand right now, we have what we need to complete the pilot as long as we can continue the PETA authorization.

Ms. JACKSON LEE. Mr. Gould.

Mr. GOULD. Ma'am, thank you for the question as well. Right now, our authorities are—DHS's authorities are limited to the core 30 airports. They are very reactive and they are for a limited time, limited duration, for a very discrete event. In the future, I believe that additional authorities for other airport environments, as well as other modes of transportation, are essential. As I said before, pipelines, rail systems, major terminals, cruise ships, they are all subject to the same sort of nefarious drone activities we see at an airport. Being able to go beyond the core 30 airports to those other modes of transportation, I think, is very important. Thank you.

Ms. JACKSON LEE. Mr. Gould, I am going to continue with you because I thank you for that openness. I don't think many Members, except for your testimony, realize that you have a limitation when we have over 300 million people and the land mass that we have here in the United States. Why don't you probe that a little bit more as to how dangerous it is to leave these other elements out of oversight and the authorization that you would need.

Ms. VINOGRAD. Chairwoman, if I may just jump in for one moment. Thank you for articulating some of the gaps in existing DHS authorities. The administration will be in the very near future submitting a legislative proposal to Congress that articulates the gaps that we seek to address in the reauthorization process.

I will note that in the statutory assessment that was provided to Congress in December, the administration did review and articulate gaps that we do see, which include the proactive and persistent protection of airports by DHS. DHS currently does not have the authority to engage in that proactive and persistent activity further.

We have articulated that airports do not have the authority to, for example, purchase equipment to, unto themselves, engage in detection and mitigation of unmanned aircraft system threats. So, we look forward to submitting that legislative proposal to you and to addressing these gaps based on the escalating threat environment.

Ms. JACKSON LEE. I thank you. I think I had posed the question to Mr. Gould as to the extent of the potential danger to TSA. Mr. Gould.

Mr. GOULD. Ma'am, I agree with my colleague from the Department on where we are at on this. Drones present a threat in the airport environment and the transportation environment writ large. It is a very challenging threat. It is a very dynamic threat. The proliferation of drones are growing significantly. Detecting them, identifying friend from foe, legitimate operations from perhaps malicious operators, is a true challenge in transportation

venues. It is one that we need to address with the whole-of-Government solution. I am very pleased——

Ms. JACKSON LEE. Thank you.

Mr. GOULD [continuing]. With our emergency—oh, go ahead, ma'am, sorry.

Ms. JACKSON LEE. No, I just said thank you very much. Let me just get in a last question of how much are we fearful of terrorist utilization of these drones? Someone can quickly answer.

Ms. VINOGRAD. We are deeply concerned by the potential use of malicious threat actors including terrorist organizations related to the use of unmanned aircraft systems.

Ms. JACKSON LEE. Well, I look forward to working with the committee and working with the administration for a very important issue. I thank the witnesses for their testimony. Mr. Chairman, I thank you for your indulgence. I yield back.

Chairman CORREA. Thank you, Ms. Jackson Lee. Any other Members wish to ask questions under this first round of questioning? Seeing none, I would ask the committee if anybody would like a second run of questions? That is an affirmative. Ranking member.

Mr. GIMENEZ. It is just not a question, really. I really want to push forward with this committee looking at what we are doing as a Nation to, you know, we can detect them. We know they are there. What can we do about it, OK? We need to do—we need to work on the capabilities of doing something about it sooner rather than later. So, I would hope that this committee can have a closed session on that in the near future. Thank you.

Chairman CORREA. Mr. Gimenez, I would just comment that I concur with you. Before we get there, I would like to have that closed session with some of these folks here to get a better picture of what we are facing and what action we need to at least to begin to address the emerging threats.

Mr. GIMENEZ. If I could just make one more comment. We don't have to shoot missiles at them, OK? So, I mean, I want to get that off the table, OK? There are other ways that you can mitigate and have an offensive capability, a defensive capability against these without being missiles. I, you know, in the news, the Israelis are doing some stuff with this. Anyway, that is some of the things that we really need to look at.

Chairman CORREA. Mr. Gimenez, I totally agree with you because I think it starts out with education. Again, take care of the knucklehead factor, which are people just think it is cute to fly their drone into an airport area, which without understanding the implications after that. Then you got that criminal element. Then we go to the next level of action. Mr. Bishop, you had some questions, please.

Mr. BISHOP. Thank you, Mr. Chairman.

Chairman CORREA. Five minutes, go.

Mr. BISHOP. I am going to pursue the same avenue. I do think, to Ms. Titus' point, I certainly don't think we should be firing missiles at drones in Las Vegas. A lot of things happen in Las Vegas. I think that would be a bad modification. I see——

Chairman CORREA. Well, it would stay in Las Vegas, right?

Mr. BISHOP. It would stay in Las Vegas, I am not sure. I think we are conflating a couple pieces of this that require different responses. So, Mr. Gould, I am very sensitive to the difficulties of figuring out how to mitigate the problem of drones, both the nefarious ones and ones that are just sort-of idiots operating their drone around to take pictures around U.S. airports. I get that.

I see a very different picture in terms of cross-border flights from Mexico. So, Mr. Michelini, I will sort-of return to you. It is funny, you know, I know it is—you guys are engaged in very sophisticated business. I appreciate that you are. But we always kind-of revert to language like we are going to mitigate the threat, which doesn't really tell me what the—and then it turns out you are jamming their signal so they got to land their drone. That doesn't really seem to do it to me.

So, to Mr. Gimenez' point, I don't even know what it requires. I don't profess to be a technical expert. But I want to ask again because you have said that there are cross-border flights to bring in drones, or at least that potential exists. You said there are cross-border flights, you know, in large numbers. I can't think of a legitimate reason for a cross-border drone flight from Mexico. Now, if one goes from the United States over to that side, I really can't see why that would be either, unless they are yours.

So, what is the reason that would be legitimate for there to be a cross-border drone flight? There appear to be lots of them. Why would it be, in your judgment, reasonable to limit our policy to, at best, the mitigation you have described, which is causing that drone to land? I can tell you that I don't think if you blew up a bunch of Mexican cartel drones, particularly the heavy ones you are talking about, I don't think they would keep doing it.

Mr. MICHELINI. No. Well, first of all, you are absolutely correct that there should be no cross-border flights of small UASs, right? That is illegal. Part 107 does not allow that. The same before, you can't go above 400 feet without a waiver, and there are no cross-border flights. To use that word that you brought up, mitigation, that is what we do though. The aircraft will either flutter down to the ground where we are or return. But it is incapable then of—it is done. We have stopped that threat in that case.

Mr. BISHOP. Is it technically not possible to destroy them?

Mr. MICHELINI. I can just tell you since I have been in this program, we haven't run down that corridor yet. So, it is just something that hasn't been explored.

Chairman CORREA. Is the answer to that question one under behind closed doors? I think we can discuss it.

Mr. MICHELINI. Well, we can probably pursue. I am sure—like I am sure DOD, who has authority to do this is in a different category than us. Like again, this is a brand-new authority for us. It is only a few years old. We have taken a very careful way to go forward with it. That is exactly where we are right now. We feel pretty comfortable with where we are, and in absolutely growing these capabilities. We just haven't entertained that one.

Chairman CORREA. Thank you. I am going to recognize Mrs. Harshbarger, who would like to——

Mr. BISHOP. Mr. Chairman, could I ask one more? I have still——

Chairman CORREA. Sure.

Mr. BISHOP [continuing]. Time still here.

Chairman CORREA. OK, go ahead. Go ahead.

Mr. BISHOP. Or it was before they clicked. Just one thing further. You know, I noticed that in September of last year, FAA issued a no-fly order for drones for a period of time because there were so many in the air. It was really triggered—I got the impression it was directed at news organizations because they were having this influx of Haitian migrants at the time. If you can do that, why couldn't you just follow the same course and issue—get an FAA order to have no flights across the border?

Mr. MICHELINI. So the TFR, the temporary flight restriction that was set up, again, you have to appreciate that is just set up for people who are willing to participate, right? So, if you are a cartel member and you set up a no-fly zone somewhere, you wouldn't necessarily follow it. So, we are back to the category we were before where we have to detect them and mitigate the threat.

Mr. BISHOP. Thank you, Mr. Chairman.

Chairman CORREA. Thank you, Mr. Bishop. Now, again, Mrs. Harshbarger, you are recognized for 5 minutes of questions, ma'am.

Mrs. HARSHBARGER. Thank you, Mr. Chairman. I just have one other question for Mr. Michelini. You stated that you keep seeing the same offenders over and over. Are these people not being prosecuted when you do find them and you know that they are accountable for these illegal drones and illegal drug smuggling or whatever they are doing? Or are they not being prosecuted? If not, why not?

Mr. MICHELINI. They are absolutely being prosecuted. So, when we do identify a drone to mitigate or follow the response, there are a couple of actions we could take. We can run an investigation. Many times, we can track the drone and know where it is landing and taking off. Then, of course, both law enforcement on both sides of the border can act out legal proceedings. So, that is the case. We do respond and make arrests to illegal drone use.

Mrs. HARSHBARGER. So, are they being allowed to be repeat offenders again then even if they are held accountable? I guess I don't understand that part.

Mr. MICHELINI. No. So, the data point where we said there are some unique IDs that have flown—that have flown back and forth, that just means we haven't got to them yet. Once we do make arrests, then the court proceedings would go as they do.

Mrs. HARSHBARGER. OK. All right. Thank you for that. With that, I yield back, sir.

Mr. GIMENEZ. Mr. Chairman.

Ms. JACKSON LEE. Mr. Chairman.

Chairman CORREA. Ms. Sheila Jackson Lee is recognized for 5 minutes of questions. Ms. Lee.

Ms. JACKSON LEE. Yes, thank you so very much, Mr. Chairman. This is fascinating, overwhelming, and creating a sense of, I think, warranted fear. This may be a line of questioning that, Mr. Chairman, I join you in a Classified circumstance. But I would like someone to say, give me the sense of what is the depth of the problem. Meaning that is this a growing problem?

With the proliferation of baby drones that 5-year-olds are getting for Christmas presents, which may not go up more than a certain

amount, but who knows what level is purchased. What is the depth of the problem, if I can either get that from the Assistant Secretary for Counter Terrorism? As well, the depth of the problem around airports. I want to focus around the commercial flying industry and the potential for a catastrophic incident because of the proliferation of drones and whoever can take that question.

Ms. VINOGRAD. Thank you. I agree with all the adjectives that you used and more. The threat environment is escalating both in terms of scale and the scope of the threats associated with unmanned aircraft systems. Because of technological advances, as well as the low cost of these UAVs, their maneuverability, the low risk to the operator, as well as the fact that many people think they are fun, these are becoming a platform and a tool of choice. To be clear, they serve a lot of beneficial purposes.

We are very aware that because of the factors that I laid out, UAV traffic is increasing significantly. What that means is that just proportionally speaking, both unintentional hazards and maligned uses of UAVs are going to create more credible threats to DHS missions. That is why we are focused on addressing any gaps in our existing authorities. Congresswoman, you asked about airports. Thank you for asking this question. I will turn to my colleague from TSA in a moment. But we have significant data and unfortunately actual incidents that point to increasing threats to airports.

As I previously mentioned, DHS currently doesn't have the authority to engage in proactive and persistent C–UAS operations at domestic hub large airports. That was indicated in the statutory assessment that we provided to you. So, in summary, because the threats are going to increase, that logically means that the threats in and around these airports are also going to increase. We, in the legislative proposal that the administration will soon provide to Congress, very much look forward to working with all of you in addressing these critical gaps.

Mr. GOULD. Ma'am, thank you also——

Ms. JACKSON LEE. Thank you.

Mr. GOULD [continuing]. From a TSA perspective for that question. I agree with my colleague from the Department. The airport environment is where unmanned aircraft systems and commercial aircraft can just come into contact. You know, airplanes are trying to land or take off. People are flying drones around. It just is inherently a high-risk operation.

But it doesn't even have to be that close to the airport. Like I said before when Newark Liberty was shut down in 2019, the drone was at 3,500 feet over an adjacent airport, but it was high enough to interfere with a flight path for Newark Liberty. That creates issues with potential mid-air collisions. It creates problems when aircraft have to take evasive action, which happened 49 times in the past year involving 5 commercial flights as well.

But it doesn't even have to be a mid-air collision that really causes a problem. A drone incursion on an airport that was somehow militarized could create a problem with an aircraft just sitting on the ground fully fueled or being fueled. Like I said earlier, the number of incidents that we see around airports is quite staggering. The visual reports that we get are just a tiny fraction of

what technical data shows us is really occurring around the airport. It is a significant problem and one that we really do need to address.

Ms. JACKSON LEE. Mr. Chairman, thank you. I will just simply say the witnesses have been excellent and a clarion call has been made and I look forward to working with the administration and our agencies on this. I am laser-focused, if I might, on the airports and surrounding areas. I think, Mr. Gould and Ms. Vinograd, you have given us a pictorial power story that should not be cited as over-exaggeration, but a call to action because that is our obligation, both Congress and the Executive. I thank you for the future offering of this legislation, which I hope to be a part of to be able to help solve this problem and secure America's skies, as well as the American people.

Chairman CORREA. Thank you, Ms. Jackson Lee. Mr. Gimenez, you had some thoughts.

Mr. GIMENEZ. Yes, thank you again. Some more comments. Look, we do have some capabilities against piloted unmanned aircraft. But my fear is that the capabilities of these unmanned aircraft is getting more and more sophisticated. Really for nefarious purposes, they can be unpiloted and just given a mission. The drone will carry out the mission, period. You can't knock it down because it is not being—it is not communicating to anybody. It is all internal.

So, that is why I think we need to have something of a closed session and talk about these issues and then also the issues how do you actually—how can you actually, you know, knock them down? Because as you said, it is not about a mid-air collision. We can have a drone go into a—a militarized drone go into an airport and cause havoc and destruction and loss of life.

So, it is a great danger. Something that has been identified for some years and it is going to happen. You know, I am telling you it is going to happen, OK? So, you know, we need to be prepared for it, and we need to stop it in any way possible. Thank you, Mr. Chairman.

Chairman CORREA. Thank you, Mr. Gimenez. Any other Members wish to comment or question our witnesses? Seeing none, I just wanted to thank our witnesses here today. Just to remind folks that we are talking about 4,000 feet, 5,000 feet up in the air, but also another area that we should consider. That is, you know, 15 feet off the ground, back yards. More and more people at home are sitting at home Sunday afternoon in their back yards, then you have a drone come in to essentially observe what you are doing as a private citizen. These are privacy issues, and we need to address them as well.

So, with that being said, I want to thank the witnesses for their valuable testimony, and the Members for their most important questions. Mrs. Miller-Meeks, did you want to ask some questions, 5 minutes?

Mrs. MILLER-MEEKS. Yes, I would, if I can.

Chairman CORREA. Of course, please.

Mrs. MILLER-MEEKS. Thank you, Mr. Chair and Ranking Member Gimenez. Mr. Michelini, I have read reports and I have seen first-hand on trips to the border that drug cartels are using drones to facilitate movement of drugs and illegal migrants over the

Southwest Border. I know you alluded to this in your testimony. Can you describe and if it happened during my absence, I apologize, what the CBP has seen and then what capabilities do you have to counter transnational criminal and drug trafficking organizations on the border?

Mr. MICHELINI. So, what we have—so, as far as counter small UAS and what we have seen, I think you might have been out. But we had 5 near-misses just with our own aircraft and a small UAS in the last year-and-a-half. We have had 6,500 illegally cross the border since August 2021, that we have seen. Again, this is really important to, just to go what Mr. Gould is saying, it is just what you see, right? Where you have your capabilities. Then 1,700 illegal crossings since January.

The illegal crossings are just one category of it. The other category is just parking drones so you—so the cartels would create a sense of domain awareness of where they want to go. Whether that is how you cross via port of entry or how you cross between ports of entry, and then how law enforcement on the U.S. side is reacting to how you are crossing. So, it is a great tool for the cartels. You know, again, they don't have First or Fourth Amendment. They don't have any concerns, right? They are just operating at will.

So, we have developed from DHS lead a con op on how we execute counter-UAS operations on the Southwest Border. Presently, we have 2 covered locations and we will intend to expand it. All within a judicial, you know, concise process to ensure we are doing this within our authorities. It is a process and we are moving forward and I think we have had some great successes and we have had a lot to learn. It is like every other person sitting here, it is an uphill battle right now. But, you know, in a moment like this, I think there is some clarity on where we need to go.

Mrs. MILLER-MEEKS. So, given the increased usage of unmanned aerial drones from both the CBP side, U.S. side, and from the cartels, and that we have supply chain issues, is there a supply chain problem that you are experiencing in relationship to getting the equipment that you need?

Mr. MICHELINI. I am sorry, I wouldn't be aware if there is a supply chain problem on that. But I can look into that for you.

Mrs. MILLER-MEEKS. Thank you. Ms. Vinograd, the authority that Congress granted to DHS to counter UAS in certain circumstances sunsets in October 2022. Can you speak—and if you already have, again, my apologies—about DHS's plan to seek an extension of that authority?

Ms. VINOGRAD. Thank you. An expiration in DHS's authority to engage in protective measures against credible threats to the safety and security of DHS missions would result in significant risk to all of our homeland security. As such, DHS in partnership with other members of the administration, will in the very near future be providing to Congress a legislative proposal to seek reauthorization to address the elevating and escalating threat landscape.

Mrs. MILLER-MEEKS. Thank you. I look forward to seeing that document. Thank you to our witnesses and thank you, Chair. I appreciate the opportunity to ask a question. I yield back.

Chairman CORREA. Thank you, Mrs. Miller-Meeks. Anybody else want to jump in? Questions, thoughts? Seeing none, again, I thank

the witnesses for their testimony, Members for their questions. Members of the subcommittee may have additional questions for the witnesses and we ask you to respond, the witnesses, expeditiously in writing to those questions.

The Chair reminds Members that the committee's record will remain open for 10 business days. Without objection, this committee stands adjourned.

[Whereupon, at 11:40 a.m., the subcommittees were adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN BENNIE G. THOMPSON FOR SAMANTHA VINOGRAD

Question 1a. The counter-unmanned aircraft systems (C–UAS) authorities provided by Congress to DHS allow the Department to "mitigate a credible threat that an unmanned aircraft system or unmanned aircraft poses to the safety or security of a covered facility or asset."

Please explain how DHS defines a "credible threat," and how the Department assesses a credible threat?

Question 1b. What is the process for identifying and designating a "covered facility or asset"?

Question 1c. Once an unmanned aircraft system has been deemed a credible threat to a covered facility or asset, what additional approvals are needed to mitigate the threat?

Answer. Response was not received at the time of publication.

QUESTION FROM CHAIRMAN J. LUIS CORREA FOR SAMANTHA VINOGRAD

Question. I understand that DHS plans to establish uniform guidelines and policies for those in need of counter-unmanned aircraft systems (C–UAS) to request such assistance.

How has DHS engaged with stakeholders, such as critical infrastructure owners and State, local, Tribal and territorial law enforcement while developing guidelines and policies for requesting C–UAS assistance?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRWOMAN BONNIE WATSON COLEMAN FOR SAMANTHA VINOGRAD

Question 1a. In September 2019, the Secretary of Homeland Security issued the *DHS Counter-Unmanned Aircraft Systems (C–UAS) Policy Guidance,* requiring DHS components to conduct assessments to document the protection of privacy, civil rights, and civil liberties. We have heard concerns about the ways in which these authorities could impact privacy, civil rights, and civil liberties, so I want to be very clear on how DHS has used its authorities.

Please identify any instances in which DHS has used its C–UAS authorities against a drone owned or operated by a journalist or news-gathering organization.

Question 1b. Please identify any instances in which DHS has used its C–UAS authorities against a drone owned or operated by a non-journalist nonetheless engaged in an activity closely associated with the First Amendment, such as a participant of a peaceful protest or demonstration.

Question 1c. Has any individual or organization made a legal claim against DHS for utilizing C–UAS authorities in a manner that violates the Constitution, statutory or regulatory privacy or due process protections, or the Preventing Emerging Threats Act of 2018 itself? If so, please describe the circumstances.

Answer. Response was not received at the time of publication.

Question 2a. Counter-unmanned aircraft systems (C–UAS) authorities allow DHS to seize or use reasonable force to destroy any drone that poses a credible threat to a "covered facility or asset." Civil liberties groups have argued that the Preventing Emerging Threats Act of 2018 authorizes the Government to seize or destroy private property without adequate due process.

What privacy and civil liberties stakeholders has DHS collaborated with since the enactment of this Act and how often has it engaged with these stakeholders?

Question 2b. How does DHS typically mitigate drones? Does mitigation involve seizure or destruction? Please describe the mitigation process and what happens to the drone once it is on the ground.

Answer. Response was not received at the time of publication.

Question 3. The Preventing Emerging Threats Act of 2018 authorizes DHS to intercept, acquire, or access communications to or from unmanned aircraft systems (UAS) only in support of an authorized counter-unmanned aircraft systems (C–UAS) action.

Once a UAS has been intercepted and rendered safe, what is the process to gain additional information about the operator and their purpose? Has DHS sought a warrant to obtain additional information once a UAS is on the ground? If so, how many times?

Answer. Response was not received at the time of publication.

QUESTION FROM CHAIRMAN J. LUIS CORREA FOR SCOTT W. CLENDENIN

Question. According to the Federal Aviation Administration, there are currently 854,694 registered drones in the United States, including 321,370 commercial drones and 529,820 recreational drones. Although most use of unmanned aircraft systems (UAS) is lawful, such systems can be exploited for malicious use by bad actors, threatening security and public safety. The threat can take several forms, including kinetic attacks with payloads of explosives, surveillance against law enforcement, and foreign intelligence gathering, just to name a few.

Has the UAS threat been particularly more present in a specific geographic area or with a certain type of infrastructure (e.g., ports, border, etc.)?

Answer. Response was not received at the time of publication.

QUESTION FROM CHAIRMAN J. LUIS CORREA FOR AUSTIN GOULD

Question. According to the Federal Aviation Administration, there are currently 854,694 registered drones in the United States, including 321,370 commercial drones and 529,820 recreational drones. Although most use of unmanned aircraft systems (UAS) is lawful, such systems can be exploited for malicious use by bad actors, threatening security and public safety. The threat can take several forms, including kinetic attacks with payloads of explosives, surveillance against law enforcement, and foreign intelligence gathering, just to name a few.

Has the UAS threat been particularly more present in a specific geographic area or with a certain type of infrastructure (e.g., ports, border, etc.)?

Answer. Response was not received at the time of publication.

QUESTION FROM CHAIRMAN J. LUIS CORREA FOR DENNIS MICHELINI

Question. According to the Federal Aviation Administration, there are currently 854,694 registered drones in the United States, including 321,370 commercial drones and 529,820 recreational drones. Although most use of unmanned aircraft systems (UAS) is lawful, such systems can be exploited for malicious use by bad actors, threatening security and public safety. The threat can take several forms, including kinetic attacks with payloads of explosives, surveillance against law enforcement, and foreign intelligence gathering, just to name a few.

Has the UAS threat been particularly more present in a specific geographic area or with a certain type of infrastructure (e.g., ports, border, etc.)?

Answer. Response was not received at the time of publication.