SAFEGUARDING THE HOMELAND FROM UNMANNED AERIAL SYSTEMS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE

AND THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

DECEMBER 10, 2024

Serial No. 118–86

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

60–350 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
NICK LALOTA, New York
MIKE EZELL, Mississippi
ANTHONY D'ESPOSITO, New York
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
ERIC SWALWELL, California
J. LUIS CORREA, California
TROY A. CARTER, Louisiana
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
GLENN IVEY, Maryland
DANIEL S. GOLDMAN, New York
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
ROBERT MENENDEZ, New Jersey
THOMAS R. SUOZZI, New York
TIMOTHY M. KENNEDY, New York
LAMONICA MCIVER, New Jersey
YVETTE D. CLARKE, New York

STEPHEN SIAO, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE

AUGUST PFLUGER, Texas, *Chairman*

DAN BISHOP, North Carolina
TONY GONZALES, Texas
ANTHONY D'ESPOSITO, New York
ELIJAH CRANE, Arizona
MARK E. GREEN, MD, Tennessee *(ex officio)*

SETH MAGAZINER, Rhode Island, *Ranking Member*
J. LUIS CORREA, California
DANIEL S. GOLDMAN, New York
THOMAS R. SUOZZI, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*

MICHAEL KOREN, *Subcommittee Staff Director*
BRITTANY CARR, *Minority Subcommittee Staff Director*

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

CARLOS A. GIMENEZ, Florida, *Chairman*

CLAY HIGGINS, Louisiana
NICK LALOTA, New York
LAUREL M. LEE, Florida
MARK E. GREEN, MD, Tennessee *(ex officio)*

SHRI THANEDAR, Michigan, *Ranking Member*
ROBERT GARCIA, California
TIMOTHY M. KENNEDY, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*

VACANCY, *Subcommittee Staff Director*
ALEX MARSTON, *Minority Subcommittee Staff Director*

CONTENTS

SAFEGUARDING THE HOMELAND FROM UNMANNED AERIAL SYSTEMS

Tuesday, December 10, 2024

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM, LAW ENFORCEMENT, AND INTELLIGENCE, AND THE SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY,
Washington, DC.

The subcommittees met, pursuant to notice, at 2:34 p.m., in room 310, Cannon House Office Building, Hon. August Pfluger (Chairman of the subcommittee) presiding.

Present: Representatives Pfluger, Gimenez, Bishop, Higgins, Gonzales, LaLota, D'Esposito, Crane, Green, Magaziner, Correa, Thanedar, and Kennedy.

Also present: Representatives Malliotakis and Smith.

Mr. PFLUGER. The Committee on Homeland Security, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence, and Subcommittee on Transportation and Maritime Security will come to order.

Without objection, the gentlewoman from New York, Ms. Malliotakis, and the gentleman from New Jersey, Mr. Smith, are permitted to sit on the dais and ask questions of the witnesses.

The purpose of this hearing is to receive testimony from expert witnesses from the Federal Government and as well as the private sector about the growing threat of unmanned aerial systems, more commonly known as UAS or drones.

We will hear from two panels today, and our first panel consists of 3 witnesses from the Federal Government.

Good afternoon. I would like to welcome you all to today's important hearing on the threats posed by unmanned aircraft or aerial systems, UAS or drones and the threat to U.S. national security and the policy solutions that could mitigate these risks.

Before we begin, I would like to personally recognize 2 individuals, Congresswoman Dan Bishop and Congressman Anthony D'Esposito, for their service to the subcommittee and to our Nation, and I wish them well in their future endeavors.

As we sit here today, we're at a critical juncture in the evolution of military technology, commercial innovation, and cybersecurity. UAS have become a transformative force. They have been used in countless positive ways that include revolutionizing many industries like agriculture, logistics, film production, and others while

also improving capabilities for humanitarian relief and law enforcement.

However, as with any powerful technology, UAS have also introduced significant security challenges. In recent years the proliferation of UAS both domestically and abroad has raised serious concerns regarding the potential misuse and criminal activities, espionage and, more alarmingly, in threats to U.S. national security. From foreign adversaries seeking to exploit UAS for surveillance and intelligence gathering to the growing risk of UAS being weaponized to attack critical infrastructure, sports stadiums, our vulnerabilities are clear.

The risks posed by commercial and military grade UAS in the hands of rogue states, non-state actors, terrorist organizations, and even individuals cannot be overstated. There have already been several troubling incidents where UAS have been used to penetrate air space comprising not only our national security but public safety.

Threats to our homeland can also derive from the manufacturing of products that Americans frequently use. A glaring example is the wide-spread use of drones manufactured by Da-Jiang Innovations, DJI, a Chinese company whose products are deeply embedded in U.S. industries and critical sectors. These systems raise national security including risk of unauthorized data access and systemic vulnerabilities.

Multiple U.S. departments and agencies have already admonished against or banned the procurement of certain UAS originating in the People's Republic of China in recognition of the threats they pose. Just this past October reports indicated that CBP is blocking the importation of some UAS produced by DJI due to potential violations of the Uyghur Forced Labor Prevention Act which is a law that prohibits the importation of goods into the United States produced in whole or in part with forced labor out of the PRC.

We must work to protect U.S. communications equipment while strengthening U.S. supply chains by ensuring foreign manufactured technologies that pose security threats cannot operate in U.S. networks. The threats posed by UAS continues to present challenges.

The U.S. border is one of the most significant vulnerabilities when it comes to this type of threat. UAS have already been used to circumvent traditional border security measures such as fences, walls, and surveillance towers. UAS have been used to smuggle drugs and weapons across the border and surveil CBP locations for human smugglers to then evade detection.

CBP officials have consistently raised concerns that Mexico narco-terrorist gangs are using weaponized UAS only a short distance from the U.S. border and in many cases operating inside the United States.

UAS also pose a significant threat to critical infrastructure, including power grids, oil refineries, airports, water treatment plants, and transportation systems. A single UAS carrying explosives could potentially cause wide-spread damages, interrupt services, and result in significant economical loss to our homeland.

Additionally, recent events illustrate the diverse roles UAS have played in both state-on-state conflict and asymmetric engagements such as those in Ukraine and Israel as well as their use in potential intelligence-gathering operations near sensitive military installations at home and abroad. We must learn from these conflicts to help protect our homeland security.

DHS and DOJ were given counter-UAS authorities as part of the Preventing Emerging Threats Act of 2018 which became law as part of the FAA Reauthorization Act of 2018. The current authorities provided under the act are set to expire on December 20, 2024, just 1 week from now.

Over the past years DHS and DOJ have used these authorities to engage in activities to protect covered facilities and assets against credible threats posed by UAS, not withstanding laws such as the Wiretap Act or the Aircraft Sabotage Act that could otherwise limit such activities.

It is imperative that we not only make sure that the current authorities are extended to protect our national security but also work together to responsibly reform the current legal authorities that provide Federal agencies with critical tools to mitigate credible threats posed by UAS.

I would like to applaud Chairman Green as well as Ranking Member Thompson for their bipartisan work alongside Members on T&I and Judiciary for introducing H.R. 8610, the Counter-UAS Authorities Security Safety and Reauthorization Act of 2024. This legislation will renew and reform current counter-UAS legal authorities. The legislation will also modify and improve counter-UAS authorities of the Federal Aviation Administration, enhance important protections for the civil liberties of Americans using UAS in a legal and responsible manner, and strengthen public safety in communities throughout this Nation.

For instance, the legislation requires DHS to establish a counter-UAS mitigation pilot program under which selected State and covered law enforcement agencies may operate approved counter-UAS mitigation systems and mitigate unauthorized UAS operations on behalf of covered entities at a number of sites each.

Today we are going to hear from experts in the fields of national security, law enforcement, defense, and technology who will provide insights into the threats posed by the UAS and family of systems to our homeland and efforts to address these challenges.

I just want to say, if you are watching the news today, we have had several incidents that have occurred and are occurring right now in places like New Jersey. Recently we had an incident at Langley Air Force Base. The threat is real.

This hearing I think will address many topics. Maybe we don't have all of the answers that come out of this hearing, but my hope is that by having this hearing, by asking both the Government and non-Governmental panel, that we can get to the right questions, and we can—if we don't have the right policies in place, then let's get those policies in place. If we do and the authorities are there, then let's figure out what we can continue to do to keep our homeland safe.

There are many aspects of this, but the most important aspect is the safety and the security of every American citizen and the life that we live here.

I look forward to hearing from our distinguished panels today and working in a bipartisan manner.

[The statement of Chairman Pluger follows:]

STATEMENT OF CHAIRMAN AUGUST PFLUGER

DECEMBER 10, 2024

Good afternoon. I would like to welcome you all to today's important hearing on the threats posed by Unmanned Aircraft Systems (UAS), or drones,[1] to U.S. national security, and the policy solutions that could mitigate these risks.

Before we begin, I would like to personally recognize 2 individuals, Congressman Dan Bishop and Congressman Anthony D'Esposito, for their service to this subcommittee and our Nation. I wish them well in their future endeavors.

As we sit here today, we are at a critical juncture in the evolution of military technology, commercial innovation, and cybersecurity. UAS have become a transformative force.

They have been used in countless positive ways that include revolutionizing industries like agriculture, logistics, and film production, while also improving capabilities for humanitarian relief and law enforcement.

However, as with any powerful technology, UAS have also introduced significant security challenges.

In recent years, the proliferation of UAS both domestically and abroad, has raised serious concerns regarding their potential misuse in criminal activities, espionage, and more alarmingly, in threats to U.S. national security.

From foreign adversaries seeking to exploit UAS for surveillance and intelligence gathering, to the growing risk of UAS being weaponized to attack critical infrastructure, sports stadiums, our vulnerabilities are clear.

The risk posed by commercial and military-grade UAS in the hands of rogue states, non-state actors, and even terrorist organizations cannot be overstated. There have already been several troubling incidents where UAS have been used to penetrate air space, compromising not only national security but public safety.

Threats to our homeland can also derive from the manufacturing of products that Americans frequently use.

A glaring example is the wide-spread use of drones manufactured by Da Jiang Innovations (DJI), a Chinese company whose products are deeply embedded in U.S. industries and critical sectors. These systems raise national security concerns, including risks of unauthorized data access and systemic vulnerabilities.[2]

Multiple U.S. departments and agencies have already admonished against or banned the procurement of certain UAS originating in the People's Republic of China, in recognition of the threats they pose.

Just this past October, reports indicated that CBP is blocking the importation of some UAS produced by DJI due to potential violations of the Uyghur Forced Labor Prevention Act, which is a law that prohibits the importation of goods into the United States produced, in whole or in part, with forced labor out of the People's Republic of China.

We must work to protect U.S. communications equipment, while strengthening U.S. supply chains by ensuring foreign-manufactured technologies that pose security threats, cannot operate in U.S. networks.

The threats posed by UAS continues to present challenges.

---

[1] An unmanned aircraft is defined in U.S. Code as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. An unmanned aircraft system (UAS), or drone, generally refers to the entire drone system, including both the unmanned aircraft and ground control unit. As such, an unmanned aircraft is generally considered a subpart of a UAS rather than a synonym because it only refers to the aircraft, not the entire system. See, 49 U.S.C.§ 44801(11)–(12).

[2] U.S. Dep't of Homeland Sec., Cybersecurity and Infrastructure Security Agency, Release Cybersecurity Guidance on Chinese-Manufactured UAS for Critical Infrastructure Owners and Operators (Jan. 17, 2024), *https://www.cisa.gov/news-events/news/release-cybersecurity-guidance-chinese-manufactured-uas-critical-infrastructure-owners-and-operators.*

The U.S. border is one of the most significant vulnerabilities when it comes to this type of threat.[3] UAS have already been used to circumvent traditional border security measures, such as fences, walls, and surveillance towers.

UAS have been used to smuggle drugs and weapons across the border and surveil CBP locations for human smugglers to evade detection.

CBP officials have consistently raised concerns that Mexican narco-terrorist gangs are using weaponized UAS only a short distance from the U.S. border.

UAS also pose a significant threat to U.S. critical infrastructure, including power grids, oil refineries, airports, water treatment plants, and transportation systems.

A single UAS carrying explosives could potentially cause wide-spread damage, interrupt services, and result in significant economic losses to our homeland.

Additionally, recent events illustrate the diverse roles UAS have played in both state-on-state conflict and asymmetric engagements, such as those in Ukraine and Israel, as well as their use in potential intelligence-gathering operations near sensitive military installations at home and abroad.

We must learn from these conflicts to help protect our homeland security.

DHS and DOJ were given counter-UAS (C–UAS) authorities as part of the Preventing Emerging Threats Act of 2018, which became law as part of the FAA Reauthorization Act of 2018.

The current authorities provided under the Act are set to expire on December 20, 2024.

Over the past several years, DHS and DOJ have used these authorities to engage in activities to protect covered facilities and assets against credible threats posed by UAS, notwithstanding laws such as the Wiretap Act or the Aircraft Sabotage Act, that could otherwise limit such activities.

It is imperative that we not only make sure that the current authorities are extended to protect our national security, but also work together to responsibly reform the current legal authorities that provide Federal agencies with critical tools to mitigate credible threats posed by UAS.

I'd like to applaud Chairman Green and Ranking Member Thompson for their bipartisan work, alongside Members on T&I and Judiciary for introducing H.R. 8610, the Counter-UAS Authority, Security, Safety, and Reauthorization Act of 2024.

This legislation will renew and reform current counter-UAS legal authorities.

The legislation will also modify and improve counter-UAS authorities of the Federal Aviation Administration, enhance important protections for the civil liberties of Americans using UAS in a legal and responsible manner, and strengthen public safety in communities throughout the Nation.

For instance, the legislation requires DHS to establish a counter-UAS mitigation pilot program under which selected State or covered law enforcement agencies may operate approved counter-UAS mitigation systems and mitigate unauthorized UAS operations on behalf of covered entities at a number of covered sites each.

Today, we will hear from experts in the fields of national security, law enforcement, defense, and technology, who will provide insight into the threats posed by UAS to our homeland, and efforts to address these challenges.

I look forward to hearing from our distinguished panels today and working in a bipartisan fashion to urgently address these issues.

Mr. PFLUGER. I now recognize the Ranking Member on the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence, the gentleman from Rhode Island, Mr. Magaziner, for his opening statement.

Mr. MAGAZINER. My thanks, Chairman Pfluger, for calling this important hearing and all of my colleagues for participating.

The proliferation of unmanned aircraft systems has created a technological arms race between criminals who use UAS technology to plot acts of terror, traffic fentanyl and other illegal substances, and invade the privacy of ordinary Americans and law enforcement agencies tasked with keeping our homeland safe.

Both the criminals and law enforcement agencies are innovating at a rapid rate, and it is important that the Federal Government keep up. The time has come for Congress to expand the authority

[3] Border Security Report Fiscal Year 2018. *Border Security Report Fiscal Year 2018 / U.S. Customs and Border Protection.*

of Federal, State, and local law enforcement agencies to better utilize monitoring, tracking, and signal-jamming technologies to protect critical areas, including our borders, large public events, prisons, and sensitive Government facilities while also ensuring the civil liberties of drone operators.

This is the goal of H.R. 8610, the Counter-UAS Authorities Security Safety and Reauthorization Act, authored by Chairman Green and Ranking Member Thompson which I'm proud to have cosponsored.

For years DHS, DOJ, and other agencies have briefed this committee on the threats posed by malicious and unauthorized UAS. We have seen drones shot down at airports in this country and around the world. Major sporting events have been interrupted with players rushed from the field when unauthorized drones with unknown motives entered restricted air space.

Just a few weeks ago the FBI arrested a white supremacist in Tennessee who planned to use a drone with an explosive payload to attack a power grid.

However, it must also be said that drones are useful tools for many occupations and hobbyists. They can be useful for search and rescue, navigation, agriculture, and more, and these positive aspects remind us that we must take a measured approach to the issue.

I look forward to hearing from today's witnesses about how best to balance the benefits and risks of UAS. Moreover, I hope that this hearing will help lay additional groundwork for getting H.R. 8610 over the finish line.

Thank you to our witnesses for being here today.

I yield back.

[The statement of Ranking Member Magaziner follows:]

STATEMENT OF RANKING MEMBER SETH MAGAZINER

DECEMBER 10, 2024

Proliferation of Unmanned Aircraft Systems has created a technological arms race between criminals who use UAS technology to plot acts of terror, traffic fentanyl and other illegal substances, and invade the privacy of ordinary Americans, and law enforcement agencies tasked with keeping our homeland safe.

Both criminals and law enforcement agencies are innovating at a rapid rate, and it is important that the Federal Government keep up.

The time has come for Congress to expand the authority of Federal, State, and local law enforcement agencies to better utilize monitoring, tracking, and signal-jamming technologies to protect critical areas, including our borders, large public events, prisons and sensitive Government facilities, while also ensuring the civil liberties of drone operators.

This is the goal of H.R. 8610, the "Counter-UAS Authority Security, Safety, and Reauthorization Act," authored by Chairman Green and Ranking Member Thompson—which I am proud to have co-sponsored.

For years, DHS, DOJ, and other agencies have briefed this committee on the threats posed by malicious and unauthorized drones.

We have seen drones shut down airports in this country and around the world. Major sporting events have been interrupted with players rushed from the field when unauthorized drones with unknown motives entered restricted air space.

And just a few weeks ago, the FBI arrested a white supremacist in Tennessee who planned to use a drone with an explosive payload to attack the power grid.

However, it should also be said that drones are useful tools for many occupations and hobbyists—they can be used for photography, search and rescue, navigation, and agriculture. These positive aspects remind us that we must take a measured approach to this issue.

I look forward to hearing from today's witnesses about how best to balance the benefits and risks of unmanned aerial systems. Moreover, I hope that this hearing will lay additional groundwork for getting H.R. 8610 over the finish line.

Mr. PFLUGER. I thank the gentleman.

The Chair now recognizes the Chairman of the Subcommittee on Transportation and Maritime Security, the gentleman from Florida, Mr. Gimenez, for his opening statement.

Mr. GIMENEZ. Thank you, Mr. Chairman.

Today we are examining the growing threats posed by unmanned aerial systems, UAS or drones, and exploring solutions to better protect our homeland from this evolving technology.

The popularity and accessibility of drones have skyrocketed in recent years today. There are more than 880,000 registered drone operators in the United States with countless others operating drones without proper registration or training. While many of these operators use drones for legitimate purposes, recreational, commercial, or otherwise, there's an undeniable threat from those who misuse this technology either through ignorance of the rules and regulations or with malicious intent.

Uninformed operators can inadvertently disrupt air traffic or encroach on sensitive areas creating safety risks that strain our law enforcement and the aviation systems. While uninformed operators presents a risk, their potential impact is negligible compared to the dangers posed by nefarious actors with malicious intent. Nefarious actors, including transnational criminal organizations, terrorists, and foreign adversaries can exploit drones to evade traditional security measures, gather intelligence, smuggle contraband, disrupt transportation systems, or even launch attacks on our homeland.

The threat from nefarious actors is both real and escalating. Along our borders drones are increasingly employed by cartels to smuggle drugs and surveil law enforcement operations. We must consider all appropriate actions to ensure that foreign adversaries like the Chinese Communist Party are not using drones under the guise of legitimate activities to relay sensitive information back to China or other entities that seek to harm the United States.

Critical infrastructure such as airports, power plants, and ports face growing risks from rogue drones capable of conducting surveillance, causing disruptions, or carrying out acts of sabotage.

These risks are not hypothetical. Since 2021, the Transportation Security Administration has documented nearly 2,000 drone sightings near U.S. airports with major airports experiencing drone incursions almost daily.

Furthermore, between 2021 and 2022, the FBI reported 235 incidents of suspicious drone flights at or near chemical plants in Louisiana. Similar UAS activity is also observed at oil storage facilities in Oklahoma and natural gas facilities in Texas, highlighting the growing threat to critical energy infrastructure.

Beyond our borders the conflict in Ukraine has highlighted the weaponization of drones in modern warfare. Both sides have employed drones for reconnaissance, targeting, and direct attacks underscoring the ability to use drones to transform the dynamics of conflict.

These lessons, both from domestic incidents and international conflicts, should serve as a wake-up call for us to bolster our defenses against the misuse of drones within the United States.

Looking ahead, the stakes will only continue to rise with major global events such as the 2026 FIFA World Cup of which many games will be played in my home town of Miami and the 2028 Summer Olympics coming to the United States. We must be ready to confront these threats to safeguard critical infrastructure and ensure the safety of travelers, participants, and spectators. We have a responsibility to defend against drone threats, and the need for action is clear. We must act swiftly.

Today's hearing is an opportunity to better understand the full scope of the challenges posed by drones and to explore innovative solutions to mitigate these risks.

I want to thank my colleague from Texas, Representative Pfluger, as well as my colleagues from the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence for partnering with us to host this important hearing.

Thank you to our witnesses, Deputy Executive Assistant Commissioner Jones, Deputy Assistant Attorney General Wiegmann, and Assistant Director Wheeler for appearing before the subcommittees.

I look forward to hearing about how we can better counter rogue drones, safeguard critical infrastructure, and ensure our policies keep pace with this evolving technology.

I yield back.

[The statement of Chairman Gimenez follows:]

STATEMENT OF CHAIRMAN CARLOS A. GIMENEZ

Today, we are examining the growing threats posed by unmanned aerial systems (UAS), or drones, and exploring solutions to better protect our homeland from this evolving technology.

The popularity and accessibility of drones have skyrocketed in recent years. Today, there are more than 880,000 registered drone operators in the United States, with countless others operating drones without proper registration or training.

While many of these operators use drones for legitimate purposes—recreational, commercial, or otherwise—there is an undeniable threat from those who misuse this technology, either through ignorance of the rules and regulations or with malicious intent.

Uninformed operators can inadvertently disrupt air traffic or encroach on sensitive areas, creating safety risks that strain our law enforcement and aviation systems.

While uninformed operators present a risk, their potential impact is negligible compared to the dangers posed by nefarious actors with malicious intent.

Nefarious actors—including transnational criminal organizations (TCOs), terrorists, and foreign adversaries—can exploit drones to evade traditional security measures, gather intelligence, smuggle contraband, disrupt transportation systems, or even launch attacks on our homeland.

The threat from nefarious actors is both real and escalating. Along our borders, drones are increasingly employed by cartels to smuggle drugs and surveil law enforcement operations.

We must consider all appropriate actions to ensure that foreign adversaries, like the Chinese Communist Party, are not using drones under the guise of legitimate activities to relay sensitive information back to China or other entities that seek to harm the United States.

Critical infrastructure, such as airports, power plants, and ports, face growing risks from rogue drones capable of conducting surveillance, causing disruptions, or carrying out acts of sabotage.

These risks are not hypothetical—since 2021, the Transportation Security Administration has documented nearly 2,000 drone sightings near U.S. airports, with major airports experiencing drone incursions almost daily.

Furthermore, between 2021 and 2022, the FBI reported 235 incidents of suspicious drone flights at or near chemical plants in Louisiana. Similar UAS activity was also observed at oil storage facilities in Oklahoma and natural gas facilities in Texas, highlighting the growing threat to critical energy infrastructure.

Beyond our borders, the conflict in Ukraine has highlighted the weaponization of drones in modern warfare. Both sides have employed drones for reconnaissance, targeting, and direct attacks, underscoring the ability to use drones to transform the dynamics of conflict.

These lessons, both from domestic incidents and international conflicts, should serve as a wake-up call for us to bolster our defenses against the misuse of drones within the United States.

Looking ahead, the stakes will only continue to rise. With major global events such as the 2026 FIFA World Cup, of which many games will be played in my home town of Miami, and the 2028 Summer Olympics coming to the United States, we must be ready to confront these threats to safeguard critical infrastructure and ensure the safety of travelers, participants, and spectators.

We have a responsibility to defend against drone threats, and the need for action is clear—we must act swiftly.

Today's hearing is an opportunity to better understand the full scope of the challenges posed by drones and to explore innovative solutions to mitigate these risks.

I want to thank my colleague from Texas, Representative Pfluger, as well as my colleagues from the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence, for partnering with us to host this important hearing.

Thank you to our witnesses, Deputy Executive Assistant Commissioner Jones, Deputy Assistant Attorney General Wiegman, and Assistant Director Wheeler, for appearing before the subcommittees.

I look forward to hearing about how we can better counter rogue drones, safeguard critical infrastructure, and ensure our policies keep pace with this evolving technology.

Mr. PFLUGER. The Chair now recognizes the Ranking Member of the Subcommittee on Transportation and Maritime Security, the gentleman from Michigan, Mr. Thanedar, for his opening statement.

Mr. THANEDAR. Good afternoon. Thank you to both gentlemen and Ranking Member Magaziner for holding today's hearing as well as to our witnesses for joining us.

Over the past few years, the use of unmanned aerial systems, also known as drones, has become common across a wide range of applications. Drones have become increasingly affordable and useful within agriculture, law enforcement, search and rescue, photography, and other industries. However, as the air space becomes more and more crowded with unmanned aircraft, we must ensure the Government is prepared and empowered to protect the safety and security of U.S. critical infrastructure and the American public.

In 2018, Congress enacted initial authorities for the Executive branch to begin testing and operating counter-drone technologies, also known as C–UAS technologies. Those authorities have kickstarted the interagency coordination and technology development needed to carry out such a complex effort, but the authorities remain limited and have relied on 1 short-term extension after another.

I hope Congress will act early next year to advance legislation to extend and expand these authorities. As we do so, we must ensure the Government's counter-drone activities appropriately protect privacy and civil liberties and do not have unintended impacts on the safety of the national airspace.

As Ranking Member of the Transportation and Maritime Security Subcommittee, I am especially interested in making sure airports are protected from threats exposed by drones. Already we have seen major airport shutdowns due to errant drones causing significant delays.

Introducing new technologies that affect radio signals is especially sensitive within the airport environment and other urban environment, so we must ensure such technologies are carefully tested.

I look forward to hearing from our witnesses today about how Congress can push our counter-drone efforts into a new phase in a major yet meaningful manner.

Again, I thank our witnesses and my colleagues.

I yield back.

[The statement of Ranking Member Thanedar follows:]

STATEMENT OF RANKING MEMBER SHRI THANEDAR

DECEMBER 10, 2024

Over the past few years, the use of unmanned aerial systems—also known as drones—has become common across a wide range of applications.

Drones have become increasingly affordable and useful within agriculture, law enforcement, search-and-rescue, photography, and other industries.

However, as the air space becomes more and more crowded with unmanned aircraft, we must ensure the Government is prepared and empowered to protect the safety and security of U.S. critical infrastructure and the American public.

In 2018, Congress enacted initial authorities for the Executive branch to begin testing and operating counterdrone technologies, also known as CUAS technologies.

Those authorities have kickstarted the interagency coordination and technology development needed to carry out such a complex effort, but the authorities remain limited and have relied on one short-term extension after another.

I hope Congress will act early next year to advance legislation to extend and expand these authorities.

As we do so, we must ensure the Government's counterdrone activities appropriately protect privacy and civil liberties and do not have unintended impacts on the safety of the national air space.

As Ranking Member of the Transportation and Maritime Security Subcommittee, I am especially interested in making sure airports are protected from threats posed by drones.

Already, we have seen major airports shut down due to errant drones, causing significant delays.

Introducing new technologies that affect radio signals is especially sensitive within the airport environment and other urban environments, so we must ensure such technologies are carefully tested.

I look forward to hearing from our witnesses today about how Congress can push our counterdrone efforts into a new phase in a measured yet meaningful manner.

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

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

DECEMBER 10, 2024

In June, Democrats and Republicans in the House came together to introduce legislation to extend and expand the Federal Government's counter-drone authorities, which were first authorized in 2018.

H.R. 8610, the Counter-UAS Authority Security, Safety, and Reauthorization Act of 2024, as amended, would extend these critical national security authorities for until October 2029 and, importantly, increase privacy and civil liberty protections.

I was proud to have worked with my colleagues on both sides of the aisle on the legislation and pleased to see it advanced through the Transportation and Infrastructure Committee.

Although it looks like the bill won't get across the finish line this year, I hope that the relevant committees will prioritize moving it early next Congress.

Due to the increasingly common usage of drones, it is critical that Federal agencies can protect certain facilities and assets from nefarious unmanned aircraft systems.

Just last month, in Tennessee, a white supremacist extremist planned to attack a power grid with an explosive drone.

If the attack had been successful, it could have left thousands of Americans without power and disrupted critical services, including financial, transportation, and emergency services.

And this is just one example of malicious uses of drones.

At the same time, ensuring that Federal agencies' counterdrone activities uphold Americans' Constitutional rights to privacy, civil rights, and civil liberties is just as important.

Backyard hobbyists use drones for recreational purposes, journalists use them to capture images of major news stories, and in my home State of Mississippi, we have found drones useful for surveying the damage wrought by disasters, including the 2023 tornadoes in my district.

So, we must ensure that those uses and liberties are not infringed upon.

I look forward to hearing from our witnesses about the threats posed by drones and strategies to protect U.S. critical infrastructure and the public.

Mr. PFLUGER. I am pleased to have a distinguished panel of witnesses before us today on this very important topic, and I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. PFLUGER. Thank you.

Let the record reflect that the witnesses have answered in the affirmative.

I'll now introduce the witnesses.

Mr. Keith Jones is the deputy executive assistant commissioner for Air and Marine Operations. He has over 32 years of law enforcement experience. Notably he has helped found the San Diego sector's Border Patrol search, trauma, and rescue team and was the principal primary driver of its national expansion.

Mr. Robert Wheeler Jr. serves as the assistant director of the FBI's Critical Incident Response Group. His responsibilities include providing expertise in crisis management, negotiations, hazardous devices and tactical operations, behavioral assessment, surveillance, and aviation. He joined the division in July of this year.

Mr. Brad Wiegmann serves as the deputy assistant attorney general for national security at the U.S. Department of Justice. He has spent his career as a Government attorney with legal experience at the Department of Defense, the Department of State, and at the National Security Council.

We thank all of you for being hearing today.

We will now begin with opening statements. I know that you have submitted written statements as well, and thank you for that. If you'll please adhere to the 5-minute summary of your statements.

We'll start with Mr. Jones. You're now recognized.

STATEMENT OF KEITH JONES, DEPUTY EXECUTIVE ASSISTANT COMMISSIONER OF AIR AND MARINE OPERATIONS, U.S. CUSTOMS AND BORDER PROTECTION

Mr. JONES. Thank you, Chairman.

Good afternoon. Chairman Pfluger, Ranking Member Magaziner, Chairman Gimenez, and Ranking Member Thanedar, and distinguished Members of the subcommittee. It is an honor to be here today on behalf of U.S. Customs and Border Protection to discuss the CBP authorities and capabilities dedicated to countering threats posed by the malicious use of unmanned aircraft systems commonly called UAS or drones.

Throughout my 33-year career in border security, first with U.S. Border Patrol and now Air and Marine Operations, I've witnessed transnational criminal organizations or TCOs and other malicious actors leveraging technology to circumvent U.S. law enforcement.

In recent years I devoted significant time to understanding the increasing UAS threat to border security and coordinating CBP's strategic response. Air and Marine Operations is CBP's executive agent for counter-UAS operations. We work alongside our U.S. Border Patrol and Office of Field Operation counterparts to detect, track, and mitigate the threat of these aircraft along our borders. We also collaborate with our DOJ and FBI partners on investigations, as well as CBP innovation, the DHS science and technology directorate, the Department of Defense, private industry to identify technologies that can improve our mitigation and domain awareness capabilities.

I'd like to emphasize 3 important aspects of this subject today: First, the current state of UAS threats to border security; second, how our critical authorities enable us to respond; and, finally, the importance of improving CBP's domain awareness capabilities and technology to detect and mitigate UAS threats.

First, UAS activity on the border is increasing rapidly. During a recent 6-week period CBP sensors recorded more than 6,900 drone flights within close proximity of our borders. It is these flights, particularly those in areas of high illicit activity, that present the greatest threat to the safety of CBP's front-line personnel, pose a serious collision risk to our crude aircraft, and diminish the effectiveness of our border security operations.

Although intent cannot be derived from border proximity alone, through our intelligence processes CBP has associated a large percent of these drone flights with nefarious activities on the ground.

TCOs have fully integrated UAS technology into their operations. Of most concern to CBP is the wide use of drones to conduct reconnaissance of CBP law enforcement personnel, their locations, and their activities. This technology enables smugglers to guide noncitizens or transport contraband across the border without encountering any law enforcement.

Additionally, to a lesser extent, TCOs have used drones to fly contraband over the border. Most drones have limited payload capacity. An average recreational drone can carry only a few pounds, but the potential risk is still significant. A few pounds of narcotics, specifically fentanyl, or a few pounds of explosives could cause serious harm.

The increasing use of UAS brings me to my second point. The authorities provided by Congress through the Preventing Emerging Threats Act are essential for CBP to detect and counter this serious threat. In accordance with the act, DHS policy guidance, and internal policy, CBP conducted counter-UAS operations in 10 high-

risk sectors along the Southwest and Northern Border as authorized by the DHS Secretary. Our operations targets specific threats to covered facilities or assets while safeguarding privacy, civil rights, and civil liberties.

Obtaining authorization to implement counter-UAS operations is a rigorous and precise process, requires a credible threat determination based on extensive analysis and evidence, as well as correlation with actionable law enforcement information.

Using our authorities and targeted approach, CBP mitigated 86 UAS threats at the border in fiscal year 2023 and 60 in fiscal year 2024. CBP also mitigated 16 UAS as Special Event Assessment Rating, or SEAR, events in fiscal year 2023 and 49 in fiscal year 2024. CBP has mitigated 3 unmanned aircraft systems so far in fiscal year 2025.

Finally, TCOs are rapidly obtaining larger, more maneuverable drones with a higher capacity for payloads and the ability to fly longer, higher, and farther.

We're also tracking the threat of drones used for kinetic attacks with payloads of explosives, firearms, or weapons of mass destruction. We're already seeing drug cartels in Mexico use drones to attack the military police and their rivals which means the CBP needs these critical authorities, advance technology to maintain the strategic advantage and continued commitment to achieving persistent domain awareness.

CBP is dedicated to our security mission, and with your support we will continue to counter this rapidly-evolving threat and expand our risk-based implementation of Counter-UAS operations along the border.

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

[The prepared statement of Mr. Jones follows:]

PREPARED STATEMENT OF KEITH JONES

DECEMBER 10, 2024

INTRODUCTION

Chairman Pfluger, Ranking Member Magaziner, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittees, thank you for the opportunity to discuss U.S. Customs and Border Protection's (CBP) capabilities and efforts to counter threats posed by the malicious use of unmanned aircraft systems (UAS [1] or "drones"[2]) along U.S. borders.

CBP's Air and Marine Operations (AMO) safeguards our Nation by anticipating and confronting security threats through its aviation and maritime law enforcement expertise, innovative capabilities, and partnerships at the border and beyond. AMO interdicts unlawful people and cargo approaching U.S. borders, investigates criminal networks, provides domain awareness in the air and maritime environments, and responds to contingencies and national taskings. AMO is CBP's executive agent for counter-unmanned aircraft system (C–UAS) efforts and we work closely with the U.S. Border Patrol, Office of Field Operations (OFO), and other intelligence community and law enforcement partners to identify and assess UAS threats and coordinate appropriate responses.

The modern border environment is dynamic, requiring CBP to continually adapt its strategies to counter emerging threats and shifting conditions. Transnational

[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 air space system. See 49 U.S.C. § 44801(12).

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

criminal organizations (TCOs) are increasingly expanding their influence across and beyond the Southwest and Northern Borders. These criminal organizations leverage sophisticated tactics and extensive networks and have access to nearly unlimited resources. TCOs also continually adjust their operations, implementing new tactics and techniques to circumvent law enforcement detection and interdiction. As the guardian of our Nation's borders, CBP deploys advanced technology and capabilities that enable it to adapt to emerging threats to our borders and increase its ability to detect and interdict illegal activity in the air, land, and maritime domains.

In the last 10 years, the advancements in UAS technological capabilities, combined with a compact design and affordability, have immensely expanded the use of UAS for a broad range of commercial, governmental, and recreational purposes, including transport and delivery, critical infrastructure management, agriculture, search and rescue, disaster response, public safety, coastal security, and other tasks. While CBP supports the lawful use of technology, UAS are increasingly being exploited for malicious use, threatening national security and public safety—a matter of paramount concern for CBP. The expanded use of UAS for malicious purposes requires CBP to enhance its domain awareness and detection capabilities to identify and counter these smaller and more agile threats across the border environment.

My testimony today describes the current threats to border security posed by the malicious use of UAS and how CBP uses its C–UAS authorities and capabilities to address this expanding threat. My testimony also explains the rigorous processes required to gain Department of Homeland Security (DHS) leadership and Department of Transportation (DOT)—including Federal Aviation Administration (FAA)—approval and authorization to conduct C–UAS activities, which are designed to protect privacy, civil rights, and civil liberties, and ensure aviation safety.

THREATS TO U.S. BORDER SECURITY FROM THE MALICIOUS USE OF UAS

The UAS threat in the border environment can take several forms. Throughout border regions, CBP personnel have observed UAS being used to conduct surveillance and reconnaissance of their operations, personnel, and facilities and have identified a multitude of unmanned aircraft used in furtherance of criminal activity such as smuggling, trafficking, and conveyance of illicit materials.

Along the Southwest Border especially, CBP continues to experience high numbers of incidents involving illicit use of UAS to facilitate unlawful movement of people and narcotics. During a recent 6-week period,[3] CBP recorded more than 6,900 drone flights within close proximity of the Southwest Border.[4] It is these flights, particularly those in areas of high illicit activity, that pose the greatest risk to CBP's—and our partners'—operations, personnel, and crewed aircraft. Although intent cannot be derived from border proximity alone, using its robust intelligence process, CBP has associated a large percent of these drone flights with nefarious activities on the ground.

TCOs and other malicious actors use UAS to conduct reconnaissance of CBP personnel and operations to pass information to contacts on the ground to assist such contacts in determining where to guide non-citizens or transport contraband. The use of drones for illicit cross border activity is not only wide-spread, but highly organized and integrated into TCO operations. 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.

CURRENT CBP C–UAS AUTHORITY AND OPERATIONS

Pursuant to the Preventing Emerging Threats Act of 2018, codified at 6 U.S.C. § 124n, "Protection of certain facilities and assets from unmanned aircraft," CBP conducts UAS detection and C–UAS[5] activities as part of its response to countering evolving and dynamic threats in the border environment, while ensuring the protection of privacy, civil rights, and civil liberties.

Among other things, and notwithstanding select criminal provisions from which section 124n offers relief, the Act authorizes the Secretary of Homeland Security to provide DHS personnel with certain assigned duties (i.e., certain CBP personnel), specific statutory relief necessary to perform the C–UAS protective mission. The

[3] Between October 1, 2024, and November 16, 2024.

[4] Any drone detected within 500 meters of either side of the border.

[5] 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(5). 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 including those that do not require relief from Federal criminal laws.

statute allows CBP to take certain actions to detect, identify, monitor, track, and mitigate UAS which pose 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 "covered facilities or assets" identified by the Secretary in coordination with the Secretary of Transportation[6] from credible UAS threats that relate to specific DHS mission sets, including CBP security and protection missions. The Act also authorizes protection of shared DHS and Department of Justice (DOJ) mission sets including protection of National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) events; provision for support to State, local, territorial, Tribal, or campus law enforcement (upon request of the chief executive officer of the respective State, Tribe, or territory) for mass gatherings that are limited to a specific time frame and location; and 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 the Act and the DHS Secretary's policy guidance, CBP implemented a C–UAS policy and, subsequently, its first operations plan to designate the Yuma Border Patrol Sector as a "covered facility or asset" in July 2020 after extensive discussion and review to ensure lawful and efficient operational implementation. CBP is committed to conducting its C–UAS activities with precision, identifying and targeting illicit activity while safeguarding lawful commercial and recreational drone use.

Currently, CBP conducts C–UAS operations under 6 U.S.C. § 124n in 10 high-risk sectors along the Southwest and Northern Borders which have received covered facility or asset designation. These operations target-specific credible threats rather than persistent, wide-spread use across all border regions. Authorization for CBP C–UAS operations requires a risked-based assessment which involves evaluating threat information to include extensive analysis and evidence of threats against the covered facility or asset, including reports of visual observations and correlation with actionable law enforcement information. All C–UAS operations are required to adhere to applicable statutory and policy parameters to ensure operational integrity and compliance with all legal restrictions and privacy protections. Additionally, all CBP C–UAS operators attend a 5-day training course that includes instruction on legal parameters and restrictions.

C–UAS operations are an essential border security capability to address evolving UAS threats. CBP implemented its risk-based C–UAS approach within a framework that ensures rigorous analysis, interagency coordination, and clear documentation of a credible threat to identify and target nefarious operators and devices amongst the increasing amount of drone traffic. Using this approach, CBP mitigated[7] 86 UAS at the border in fiscal year 2023 and 60 UAS in fiscal year 2024. CBP also mitigated 16 UAS at SEAR events in fiscal year 2023 and 49 in fiscal year 2024. CBP has mitigated 3 UAS so far in fiscal year 2025.[8]

C–UAS authorities will become even more critical as the UAS threat evolves. All evidence indicates that TCOs are pursuing the use of larger drones with more maneuverability, more payload capacity, and greater capability to fly longer, higher, and farther. CBP needs these critical authorities to be extended beyond the current termination date of December 20, 2024, along with the latest C–UAS equipment, to continue efforts to counter these rapidly-evolving threats and expand risk-based implementation of C–UAS operations to additional locations along the Southwest and Northern Borders.

C–UAS POLICY AND AUTHORIZATION PROCESS

To standardize the application of C–UAS authorities, DHS established a C–UAS Program Management Office (PMO) within the Office of Strategy, Policy, and Plans (PLCY). The PMO coordinates CBP's C–UAS activities to ensure alignment with De-

[6] Defined in the Preventing Emerging Threats Act as any facility or 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 air space, through a risk-based assessment; is located within the United States; and directly relates to a select authorized DHS mission, or authorized joint DHS or DOJ mission, See 6 U.S.C. § 124n(k)(3).

[7] Generally, mitigation involves disrupting the signal between a drone and its controller, causing the drone to activate its pre-programmed recovery protocol, such as returning to its designated "home" location or hovering in place. If this action does not neutralize the threat, certain C–UAS systems can emulate the controller to redirect the drone to a secure or DHS-preferred location.

[8] As of November 16, 2024.

partmental policy and serves as the primary liaison for interagency partners, particularly DOT and the FAA.[9]

Obtaining operational authorization to deploy C–UAS technology in support of CBP's border security mission requires a rigorous assessment and the use of an established approval process so that the potential safety risks to the National Airspace System (NAS) associated with the use of such technology can be appropriately mitigated. These assessments identify covered facilities or assets and consider traditional risk elements such as threats, vulnerabilities, and consequences. These assessments also include FAA evaluation of collateral risks to the NAS, including potential interference with airport communications and aircraft navigation systems, and whether temporary flight restrictions or other measures are necessary. When coordination and deconfliction requirements are complete, DHS and FAA sign a coordination memorandum, then complete a rigorous internal review and oversight processes before the DHS Secretary designates the facility or asset as a "covered facility or asset" pursuant to the Act, a prerequisite for CBP to take C–UAS actions. This collaborative approach enables DOT, including the FAA, to preserve aviation safety, enables security experts and professionals to perform their protective security mission, and enables senior DHS leadership visibility into C–UAS operations.

PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS

In the conduct of all its operations, CBP is committed to protecting the civil rights, civil liberties, and personal privacy of citizens and visitors, as well as conducting operations with openness and accountability.

Pursuant to the Act, CBP may intercept or acquire command-and-control communications from a UAS, but only to the extent necessary to support C–UAS actions authorized by the DHS Secretary to protect a designated covered facility or asset. CBP 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 applicable Federal laws and Department policies. In addition to those privacy protections in the Act, DHS 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 DHS 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 has published multiple C–UAS PIAs for public consumption consistent with requirements outlined in the Homeland Security Act of 2002.[10]

CBP seeks to ensure that C–UAS activities collect only information authorized by law and necessary to identify and address UAS threats. CBP policies include measures to respect the lawful use of UAS without compromising the protection of a covered facility or asset. These policies continually undergo review and revision based on lessons learned and to ensure consistency with DHS policy guidance.

THE FUTURE LANDSCAPE OF UAS THREATS

Opportunities for TCOs and other threat actors to leverage drone technology will only expand. Advancements like multi-drone control, autonomous flight plans, obstacle avoidance, extended communication ranges, and longer battery life necessitate continual reassessment of CBP's detection and response strategy.

DHS's—and by extension, CBP's—statutory authority to conduct C–UAS operations to mitigate threats posed by UAS to a covered facility or asset terminates on December 20, 2024. Therefore, we look forward to working with Congress on expeditious reauthorization of this authority.

We appreciate the support we have received from your subcommittees, whose commitment to the security of the American people has enabled the continued deployment of advanced technology and capabilities that CBP needs to secure the border.

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

Mr. PFLUGER. Thank you, Mr. Jones.

The Chair now recognizes Mr. Wheeler for his opening statement of 5 minutes.

---

[9] The FAA is statutorily responsible for the safe and efficient management of the navigable air space of the United States.

[10] See, e.g., *https://www.dhs.gov/publication/dhsallpia-085-counter-unmanned-aircraft-systems-C–UAS.*

STATEMENT OF ROBERT W. "WES" WHEELER, JR., ASSISTANT DIRECTOR, CRITICAL INCIDENT RESPONSE GROUP, FEDERAL BUREAU OF INVESTIGATION

Mr. WHEELER. Thank you. Good afternoon, Chairman Pfluger, Chairman Gimenez, Ranking Member Magaziner, Ranking Member Thanedar, other distinguished Members of the committee. Appreciate the opportunity to testify on behalf of the FBI.

I currently serve as the assistant director of our Critical Incident Response Group in Quantico, Virginia. I've done that since July as you mentioned. In that capacity I lead the FBI's efforts regarding both our pre-crisis planning and response to critical incidents and major investigations, which includes responsibility for our counter-unmanned aircraft program.

As UAS use continues to rapidly grow among the public commercial and military and law enforcement sectors, this technology also lends itself to increase malicious use by state, non-state, and lone actors as you know. This technology poses some unique security challenges for us. Just this year alone we've seen concerning increase in the use of UAS in the commission of crimes with the intent to cause injury to U.S. persons on U.S. soil.

A Chinese national recently pled guilty to 2 misdemeanor counts for using a UAS to conduct espionage at a U.S. Naval facility in January. We believe UAS are being flown for similar purposes over sensitive facilities across the United States.

Just last month a subject was arrested and charged in Tennessee for attempting to use a UAS with an explosive device to destroy an energy facility. That is the same case mentioned by the Ranking Member. That subject was driven by an ideology to disrupt society through the collapse of the national power grid.

Those are 2 examples of the evolving ways that UAS are being used to harm us and our interests.

With the enactment of the 2018 Preventing Emerging Threats Act, the FBI was granted the authority necessary to mitigate a range of UAS threats in the protection of special events, emergency response, Federal investigations, personnel, and facilities. Specifically the legislation authorizes DOJ and our partners at DHS to conduct counter-UAS operations in limited circumstances to identify, track, and mitigate credible threats.

I'd stress the importance for reauthorization of the counter-UAS authority that as you know expires December 20. Failure to extend the authorities beyond then would cause significant impacts on our ability to protect the public.

A durable extension is also extremely important. Our experience has taught us that short-term extensions to counter-UAS authority effectively prevent the bureau and our partners from budgeting and staffing it in ways which would allow us to execute a long-term strategy. We know that Congress is considering extensions of 5 years or more, and we thank you for that consideration.

The FBI strongly supports pursuing expanded counter-UAS authorities for State, local, Tribal, and territorial partners as robustly and swiftly as prudently possible. SLTT partners have repeatedly informed us that existing counter-UAS authorities are inadequate.

Since our counter-UAS authority was granted in 2019, the FBI has adopted 69 operational missions using its authority and pro-

vided limited support to 121 other events. We've detected over 1,000 UAS in violation of Federal law during these missions. One example, at the Boston Marathon this past April, our team mitigated a UAS threat which resulted in the capture and prosecution of a subject.

The FBI cannot alone protect the over 40,000 Special Event Assessment Rating, or SEAR, events annually held in the United States along with the countless other requests for counter-UAS support at mass gatherings. The use of counter-UAS to protect against this situation is crucial and can only be fully addressed by expanding the capability to include our State and local partners.

In closing, we will remain committed to protect Americans by countering the malicious use of this technology. The reauthorization or long-term extension of this legislation is central to continue our mission in combatting the evolving threat. We look forward to working with you in establishing sustainable strategies to mitigate the threat going forward.

Thank you.

[The joint prepared statement of Mr. Wheeler and Mr. Wiegmann follows:]

JOINT PREPARED STATEMENT OF ROBERT W. "WES" WHEELER, JR. AND BRAD WIEGMANN

DECEMBER 10, 2024

Good morning, Chairman Pfluger, Chairman Gimenez, Ranking Member Magaziner, Ranking Member Thanedar, and other distinguished Members of the committee, and thank you for the opportunity to testify on behalf of the Department of Justice ("the Department" or "DOJ"). The Department is committed to continuing to protect the American people from the threat of illicit drone use, whether in the form of reckless flying over mass gatherings, contraband smuggling into correctional facilities, surveillance of sensitive Government operations, or any other illegal activity. Our current authority under the Preventing Emerging Threats Act of 2018, codified at 6 U.S.C. § 124n ("§ 124n"), is crucial but inadequate. The Department strongly supports the administration's legislative proposal to extend and expand our authorities to protect against illicit use of unmanned aircraft systems ("UAS"). The 2 pillars of this counter-UAS ("C–UAS") proposal are expanding Federal protective coverage for the most vulnerable sites—such as airports and critical infrastructure—and empowering our State, local, Tribal, and territorial ("SLTT") law enforcement partners to engage in C–UAS efforts nationwide, subject to restrictions and oversight. We look forward to discussing the details with the committee, but we believe that both pillars are necessary to address the threat.

I. THE THREAT POSED BY MISUSE OF DRONES

A. The Threat Continues to Grow

The use of UAS technology in the United States continues to grow rapidly. Along with significant benefits come significant risks. Commercial use of UAS already generates billions of dollars in economic growth. As of October 1, 2024, over 791,000 UAS in the United States are registered with the Federal Aviation Administration ("FAA") with more drones required to be registered that simply are not. Law enforcement and public safety use of UAS allows officials to perform critical missions, from accident rescues to tactical incursions, while reducing risk to personnel and the public.

Alongside these immense benefits, however, is the threat UAS pose in the hands of nation-state adversaries, terrorists, criminals, and irresponsible operators. As noted in the administration's "Domestic Counter-UAS National Action Plan" ("Action Plan"), UAS threats can take several forms, including:

- platforms designed or modified to conduct kinetic attacks using payloads of explosives, firearms, or weaponized chemical, biological, or nuclear material;
- cyber attacks against wireless devices or networks;
- espionage;

- the illicit trafficking of narcotics and contraband; and
- monitoring law enforcement activity.

Beyond use by actors with criminal intent, in some cases UAS have been used by operators without knowledge of or regard for regulatory boundaries. Those operators pose a hazard to Government operations, commercial activities, and the public.

The threat of UAS-enabled terrorist attacks remains significant. In 2016, the Federal Bureau of Investigation ("FBI") director testified that "given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering." Since that statement, the threat of weaponized UAS attacks manifested itself within the United States on 2 occasions, though fortunately we were able to disrupt the plots:

- (i) In November 2024, the Department arrested and charged Skyler Philippi of Columbia, Tennessee, with attempting to use a UAS as a weapon of mass destruction to destroy an energy facility. Philippi had conducted research on past attacks on the U.S. electrical system and allegedly concluded that attacking with firearms would not be sufficient; instead, he planned to use a UAS laden with explosives. He allegedly planned to use the UAS to attack the power grid, leaving thousands of Americans and critical infrastructure like hospitals without power. As alleged, Philippi was a self-styled "accelerationist" who hoped his actions would "shock the system" and lead to civil unrest.[1]
  - Importantly, current law does not contain clear authority for the Federal Government, SLTT law enforcement, or the private sector to mitigate or, for certain technologies, even detect UAS that threaten critical infrastructure.
- (ii) Also in November 2024, Edward Kelley of Maryville, Tennessee, was convicted of a conspiracy to murder Federal employees, in part through the planned use of weaponized drones. While awaiting trial for crimes he committed at the United States Capitol on January 6, 2021, Kelley planned an attack on the Knoxville FBI Field Office that would have used car bombs and incendiary devices appended to drones as revenge against law enforcement for his prior arrest.[2]

As we will discuss in more detail, expansion of current C–UAS authorities would enable our Federal and SLTT partners to build our collective C–UAS capabilities and awareness to better identify and thwart future similar attacks.

Espionage-by-UAS also became a domestic reality in the past year. In January 2024, Chinese national Fengyun Shi flew a UAS over the Newport News Shipbuilding—a highly secure naval shipbuilding complex in Norfolk, Virginia—and took extensive photos and videos. Shi was arrested before boarding a flight to China. He later pleaded guilty to 2 misdemeanor counts under a World War II-era statute that is part of the Espionage Act and received a 6-month sentence.[3]

UAS also continue to be used for other crimes, sometimes with fatal consequences. In October 2024, a man in Los Angeles, California allegedly used a UAS to drop off fentanyl and other narcotics to buyers, one of whom died of a fatal overdose.[4] All of these examples during this calendar year demonstrate that we must not underestimate the ingenuity of criminals to achieve their unlawful objectives using this technology.

B. The Threat Posed to Prisons

The Federal Bureau of Prisons ("FBOP") is also seeing an increase in the criminal use of UAS in the prison context. Between 2015 and 2019, the Department of Justice reported 130 drone incidents—typically involving criminals using UAS to deliver drugs, cell phones, weapons, or other contraband—in Federal prisons alone, and that count is likely low compared to actual incidents. FBOP adopted its formal UAS incursions reporting policy in 2018. After reporting instructions went into effect, the number of incidents recorded increased by 87 percent.[5] Similar incidents at State and local prisons and jails are frequent. Unlike staff at Federal facilities, SLTT correctional personnel are not covered by the C–UAS authorities provided by Congress to DOJ and the Department of Homeland Security ("DHS").

---

[1] *https://www.justice.gov/opa/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy-facility*.

[2] *https://www.justice.gov/opa/pr/federal-jury-convicts-man-conspiring-murder-fbi-employees#*.

[3] *https://www.startribune.com/u-student-from-china-receives-6-month-prison-term-for-taking-drone-photos-over-naval-shipyard/601162150*.

[4] *https://www.justice.gov/usao-cdca/pr/lancaster-man-arrested-charges-he-used-drone-fly-fentanyl-including-customer-who-later*.

[5] *https://nij.ojp.gov/topics/articles/addressing-contraband-prisons-and-jails-threat-drone-deliveries-grows*.

To note just a few recent examples, in September of this year, a man pled guilty to providing contraband, including drugs, to the Federal Correctional Complex in Yazoo City, Mississippi.[6] In August 2024, DOJ charged 23 defendants with conspiracy to use UAS to deliver methamphetamine, marijuana, and cell phones to Georgia State prisons. Operation Night Drop identified 2 networks of prison inmates and outside conspirators who used UAS and other methods to deliver large quantities of drugs, cell phones and other contraband to Smith State Prison in Glennville, Telfair State Prison in McRae-Helena, and various other Georgia State prisons.[7] Eighteen months before that, the Department brought charges against 4 men in California for a long-running conspiracy to distribute drugs and other contraband via drones at 6 California State prisons.[8] These schemes are happening with greater frequency and effect.

C. FBI Protection of Mass Gathering from the UAS Threat

When it enacted § 124n in 2018, Congress facilitated certain C–UAS missions by the DOJ and DHS, including the protection of Special Event Assessment Rating ("SEAR") events. Since the law's enactment, the FBI has conducted 139 UAS detection and C–UAS protection operations at large events, ranging from the Major League Baseball World Series to the New Year's Eve celebration in Times Square, where national defense temporary flight restrictions were in place. During those operations, the FBI detected 1,624 UAS operating in violation of Federal law, located the operator in 500 instances, and attempted technical mitigation against 129 UAS. The FBI also continues to provide protection from UAS threats at a limited number of other special events and in support of Federal investigations, including those in response to UAS incursions at military installations.

When available and appropriate, DOJ pursues criminal charges for UAS misuse at mass gatherings. For example, in February 2024, DOJ charged an individual with felonies related to flying a UAS over M&T Bank stadium during the National Football League's AFC Championship game in Baltimore, Maryland in January 2024.[9] In September 2024, a Boston man was charged with unlawfully flying a UAS in restricted National Defense Airspace when he flew his UAS near the finish line at the Boston Marathon in April 2024. The UAS flight prompted law enforcement and bomb technicians to seize the device mid-air, land it, and evaluate its threat to the public.[10]

While constituting an impressive track record that prevented or significantly minimized the impact of UAS misuse, the FBI's covered events represent only 0.05 percent of the over 240,000 special events during that time period for which potential C–UAS protection could have been authorized under 6 USC § 124n. That number makes clear that the demand for such support to protect our communities has far outstripped the Federal Government's limited resources. We cannot do this alone.

II. THE ADMINISTRATION'S CONSOLIDATED C–UAS LEGISLATIVE PROPOSAL

A. Overview of the Administration Proposal

Starting in 2021, Executive branch agencies that are confronting the growing threat from UAS collaborated to identify the critical gaps in law and policy that impede our ability to defend our national security interests and public safety from UAS threats. The product of that work was the administration's Action Plan. At the top of the Action Plan's recommendations was a recommendation to "Expand Legislative Exemptions for UAS Detection and C–UAS Mitigation Activities." The Executive branch also assembled a legislative proposal that would implement some of the recommendations and greatly improve our protections against all types of UAS misuse.

Specifically, the administration's proposal would expand the current § 124n authority in targeted ways based on our experience under the law and our assessment of the growing threat. Current § 124n authority will lapse this month, so our existing programs must be reauthorized to avoid shutting down FBI's ability to protect

---

[6] *https://www.justice.gov/usao-sdms/pr/tennessee-man-pleads-guilty-using-drone-fly-marijuana-yazoo-city-federal-correctional.*

[7] *https://www.justice.gov/usao-sdga/pr/pair-indictments-charge-conspiracies-use-drones-deliver-illegal-drugs-contraband-cell.*

[8] *https://www.justice.gov/usao-edca/pr/four-indicted-scheme-deliver-drugs-state-prisons-drone.*

[9] *https://www.justice.gov/usao-md/pr/pennsylvania-man-facing-federal-felony-charges-illegally-operating-drone-during-national.*

[10] *https://www.justice.gov/usao-ma/pr/boston-man-charged-violating-national-defense-airspace.*

mass gatherings. The authority is essential because, without it, use of the most effective types of UAS detection and C–UAS technologies could violate criminal laws, including those that prohibit destroying or disabling aircraft and intercepting signals and communications. See, e.g., 18 U.S.C. § 32 (the Aircraft Sabotage Act); 18 U.S.C. §§ 2510 et seq. (the Wiretap Act, also known as Title III); 18 U.S.C. §§ 3121–3127 (the Pen/Trap Statute).

Based on experience gained since 2018, the administration's legislative proposal would close additional gaps that currently leave us vulnerable to UAS threats. Current law makes no provision for permanent protection of transportation facilities such as civilian airports; for critical infrastructure such as power plants or oil refineries or chemical facilities; or for high-risk prisoner transports. Gaps in legal authorities leave sensitive Federal facilities, such as CIA headquarters, vulnerable to both intelligence collection by foreign states and physical attacks by hostile actors. Current law also lacks a provision to make Federal C–UAS efforts more efficient by allowing DOJ and DHS to fulfill each other's statutory missions, and those of the Departments of Defense ("DoD") and Energy ("DOE"), in exigent circumstances. Perhaps most critically, § 124n does not authorize SLTT law enforcement to engage in any kind of C–UAS activity that would otherwise violate Federal law. The absence of such authority has hamstrung their efforts. Neither DOJ nor DHS has the resources to fill the thousands of requests each year we receive to use our authority to assist our SLTT partners.

The administration's legislative proposal would fill these gaps in the following ways:

B. Authorizing Limited SLTT C–UAS Programs

(i) Authorizing SLTTs to Use Pre-Approved Detection-Only Equipment

The legislation would authorize all SLTT law enforcement as well as the owners or operators of airports or critical infrastructure to use Federally-vetted UAS detection-only capabilities, subject to conditions and safeguards. As noted above, experience has shown that the demand for protection across the country from UAS-based threats greatly exceeds the Federal Government's capacity. We need to empower SLTT law enforcement agencies across the country, which are primarily responsible for keeping our citizens safe at the local level, to take the steps needed to protect their communities from this emerging threat. We also need to allow critical infrastructure operators to take steps to protect their own facilities and assets.

Notably, the "detection-only" technology that this part of the bill would authorize would not include authority to mitigate the drone through jamming or to otherwise disrupt drones or other aircraft. Rather, the information obtained through detection of drone signals can disclose the location of the drone operator, so that law enforcement or security personnel can locate that operator and address the threat through more traditional means. The detection technology authorized for use would be tested and evaluated by DHS or DOJ, and approved by the FAA, the Federal Communications Commission ("FCC"), and the National Telecommunications and Information Administration ("NTIA") to ensure that each system does not adversely impact the national air space system. Only technologies on an approved list—maintained by DHS, in coordination with DOJ, FCC, NTIA, and FAA—could be employed consistent with the exemptions in the law. Any non-Federal entity using detection-only authority must also issue a written policy certifying compliance with the privacy protections in the bill and comply with any additional guidance issued by the Secretary of DHS or the Attorney General. This "detection-only" authority would provide significant public safety benefits and could be safely employed today.

(ii) Mitigation Pilot

The legislation would also authorize a limited pilot program for SLTT law enforcement entities, subject to a 6-year sunset provision. DOJ and DHS could designate annually up to 12 SLTT law enforcement entities to engage in both UAS detection and UAS mitigation activities, consistent with the safeguards and oversight required in the bill. Those entities would be required to receive appropriate training and vetting to enable them to both detect and mitigate UAS threats to covered facilities or assets, including mass gatherings. Because these operations could include use of more sensitive mitigation technology, all of their activities would have to be coordinated in advance with Federal partners including the FAA, which could withhold approval if the FAA identifies a risk to the national air space system from a proposed operation. Moreover, all activities would be carried out under the direct oversight of the DOJ or DHS. This is an initial step that will allow Congress, the Executive branch, and SLTT law enforcement entities to evaluate costs and benefits, learn best practices, and employ transformative technology with controls that will continue to ensure air space safety and the proper use of the radiofrequency spec-

trum through required coordination with Federal authorities. As with the detection-only authority, SLTT pilot program participants could only use equipment on an authorized list maintained by DHS, in coordination with DOJ, FCC, NTIA, and FAA.

C. Expanding Coverage to Airports and Critical Infrastructure

The legislation would also give DHS the authority to protect transportation sites, such as airports, and other critical infrastructure from UAS threats. Critical infrastructure and airports are acutely vulnerable to UAS incursions as current law makes no provision for their sustained C–UAS protection. The administration's proposed language would fix this gap and authorize Federal personnel to protect such facilities.

D. Mutual Support Authority

DHS and DOJ also currently lack the authority to assist each other, as well as DoD and DOE, with the protection of assets legally eligible for C–UAS protection. A Pentagon-led table-top exercise identified this gap as a chief impediment to fully effective Federal protection, and therefore as a key vulnerability in the U.S. C–UAS posture. The administration's proposal would ensure that DHS and DOJ are authorized to help protect the Nation's most critical and vulnerable infrastructure in exigent circumstances and when other resources are lacking.

E. Prisoner Transports

The legislation would expressly authorize the U.S. Marshals Service ("USMS") to protect high-risk prisoner transports using UAS detection or mitigation technology. Current authority covers courthouses and prisons but does not expressly address prisoner transports. The bill would close this gap and allow the use of technology where, for example, we believe there is a substantial risk involving a terrorist or organized crime figure whose confederates could use drones to attack or monitor a transport.

F. Expanding Protections for Privacy and Civil Liberties

The legislation and its implementing policies will continue to ensure that we respect privacy and Constitutional rights as we conduct our UAS detection and mitigation activities, by limiting Government actions toward protected First Amendment activities and regulating what information may be collected and shared. It is important to note that the technologies that we employ typically detect the presence of drones operating in a specific space and the only communications that are identified are the electronic data passed between the operator's controller and the UAS. Those communications direct the physical operation of the drone. The technologies used by the Department do not extract text messages, e-mail, or internet search histories from phones or tablets used to control drones, nor do they allow law enforcement to listen to voice calls. Specifically, the detection systems collect information such as the drone vendor and model; drone and controlling device serial number and media access control, or MAC, address; geolocation of the drone; location of the controller; and the most recent takeoff location and "home" location. This is much like the information required to be broadcasted by manned aircraft, and similar to that which the FAA now requires most drones to broadcast under the Remote Identification of Unmanned Aircraft rule. However, for drones that do not comply with FAA requirements, it is critical that the Government can collect the information unilaterally, exercise discretion on when to use jamming or take-over technology by seeking out the operator first (time and circumstances permitting), and make more informed decisions.

Importantly, under the proposed legislation, SLTT entities and the owners or operators of airports or critical infrastructure who operate detection technologies would be required to adhere to the same privacy protections imposed on Federal law enforcement under the existing 2018 law. Currently, any parties who operate such equipment do so without explicit legal authority and without privacy safeguards.

G. Sunset

The administration's Action Plan recommended terminating the sunset provision and permanently enacting the exemptions that Congress provided to DOJ and DHS in 2018. Terminating or significantly extending the period of these authorities would give us more certainty as we plan for the future. Experience gained over the past 4 years has demonstrated both the value of C–UAS activity by DOJ and DHS, and that these operations can be conducted safely and with strong safeguards for privacy and civil liberties. Long-term exemptions will enable us to invest more resources in this mission with confidence that it will continue far into the future. The legislative proposal retains the requirements for semi-annual briefings to specified committees, thereby ensuring appropriate Congressional oversight.

CONCLUSION

In closing, the proposed legislation by itself will not eliminate the threats presented by malicious or irresponsible use of drones. However, it will significantly enhance our ability to mitigate this threat in a manner that is measured, responsible, and consistent with the FAA mandate to integrate drones safely into the national air space system. As the United States seeks to lead the world by integrating uncrewed aviation into the national air space, Congress must build security into the frameworks that support UAS integration by ensuring that those responsible for protecting the public have the authority they need to do so. Integration and security must go together.

The provisions we have discussed are doubtless not the only possible formulation for legislation to improve on the status quo. But any successful bill should include at least some version of those 2 pillars: (i) Expanding Federal protective coverage for the most vulnerable sites—such as airports and critical infrastructure—and (ii) empowering SLTT law enforcement partners to engage in detection-focused C–UAS efforts nationwide, subject to appropriate restrictions and oversight.

We appreciate the opportunity to testify today, and we would be pleased to answer your questions.

Mr. PFLUGER. Thank you, Mr. Wheeler.

The Chair now recognizes Mr. Wiegmann for his opening statement of 5 minutes.

STATEMENT OF BRAD WIEGMANN, DEPUTY ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, DEPARTMENT OF JUSTICE

Mr. WIEGMANN. Thank you. Good afternoon, Chairman Pfluger, Chairman Gimenez, Ranking Member Magaziner, Ranking Member Thanedar, and other distinguished Members of the committee. Thank you for the opportunity to testify on behalf of the Department of Justice.

As my colleagues have just said, we are committed to continuing to work hard to protect the American people from the threat of illicit drone use, but to do so most effectively we need additional legal authority. As drones become more and more prevalent in our air space, merely continuing with our current authorities is insufficient to address the current scale of the threat.

More than 2 years ago I and others from DHS and the FAA testified before a Senate committee about this growing threat and the need for a more durable and significantly expanded legal framework. Since that time the Congress has provided extensions of existing counter-drone authority while considering how best to expand it. We are very grateful that both the House and the Senate continue to agree that this authority must not lapse.

The Department is eager to share with you the lessons gained from our experience to help reach consensus about how much and in what way to expand the existing law.

Now, the reason we need legal authority is that without it use of the most effective types of drone detection and counter-drone technologies could violate criminal laws, including those that prohibit destroying or disabling aircraft in flight and intercepting signals and communication.

As has just been said, our current authorities will lapse within the next 10 days unless reauthorized, so our first priority is for Congress to reauthorize the existing law. But I know that this committee and others have also been working on legislation to go well beyond that, and we are eager to work with Congress on a bill to help keep the American people safe.

Now, as described in our written testimony, the 2 most important issues for us are, No. 1, broadening the types of sites that law enforcement can protect from nefarious and suspicious drone uses, so, for example, to cover, as was mentioned in the opening statements, airports and critical infrastructure like power plants and chemical facilities. So we need to expand the types of sites that can be protected.

Then, No. 2, as my colleague from the FBI just mentioned, it's about empowering State and local law enforcement and operators of critical infrastructure to engage in counter-drone efforts themselves nationwide.

This is not a job the Federal Government can do alone. The FBI can only cover a tiny fraction, less than half of 1 percent, of the tens of thousands of events throughout the country each year that might need counter-drone support to protect public safety. So the demand for protection across the country just vastly exceeds available Federal resources.

To be clear, this activity can and must be done while safeguarding Americans' privacy and civil liberties. The technologies that we employ typically detect only communications being passed between the operator's controller and the drone to detect its activities—to direct its activities. They do not extract text messages, email, or internet search histories from phones or tablets used to control drones, nor do they allow law enforcement to listen to voice calls.

We collect information such as the drone vendor and model, the drone and controlling device serial number, the geolocation of the drone, the location of the controller, and the most recent take-off and home location. This is very much like the information required to be broadcast by manned aircraft and which is now required under FAA's remote ID regulation to be broadcast by drones as well. We use this information to further investigate when a crime involving a drone is suspected.

As required in current law, DOJ will continue to have guidance that contains explicit protections for privacy and civil liberties and associated training. State and local law enforcement if empowered to engage in this activity would be required to adhere to the same rules.

I appreciate the opportunity to testify today. I'd be happy to answer your questions.

Mr. PFLUGER. I thank the witnesses for their opening statements.

Members will now be recognized by order of seniority for 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized and also knowing that we have a second panel.

I now recognize myself for 5 minutes of questioning.

Let's just start with current events, and I'll ask an open-ended question. What is going on in New Jersey?

Mr. WHEELER. So, sir, the FBI in our Newark Field Office, along with the State and local partners there, are—or the bureau is actively investigating the situation you mentioned, just the unexplained sighting of drone activity over that part of New Jersey, including proximity to sensitive sites and areas of concern.

So we do not attribute that to an individual or a group yet. We're investigating, but I don't have an answer of who's responsible for that, of one or more people that are responsible for those drone flights. We're actively investigating. What the bureau has done to aid our State and local partners is what we generally do, enlist the help of the interagency, enlist the help of the public. There's a tip line there, that 1–800-CALL-FBI, tips.FBI for information from the public that could help us resolve this. It is concerning. There——

Mr. PFLUGER. Is the public at risk? Is public safety at risk? Are we concerned that there are nefarious intentions that could cause either national security or a public safety incident that would put Americans at risk?

Mr. WHEELER. There's nothing that is known that would lead me to say that, but we just don't know, and that's the concerning part.

Mr. PFLUGER. I think the fact that we have these unknown drones, UAS, that are flying over either critical or sensitive facilities is exactly why we're having this hearing.

Mr. Jones—well, actually, for anybody on the panel, let me just say, you know, we go back to last year there were incidents, including Langley Air Force Base, where for over a week we had unknown drones flying over a very sensitive military installation with F–22s and other, you know, weapon systems on the ground, and I think that was cause for concern.

So from a DHS standpoint, either on a border mission or from FBI or DOJ, you mentioned, Mr. Wheeler, we don't necessarily have the authorities we need. Why can't we take action against these drones that are flying over sensitive sites? Why are we not taking action against drones that are flying over sensitive sites?

Mr. WHEELER. So authority exists to mitigate a UAS in flight when authorized, and that could certainly apply to a sensitive site. I would be a little measured in speaking for the Department of Defense for those sites that are in question here, but I will say that we're, for the FBI, in a position, close liaison relationship with the Department of Defense and those areas that you mentioned and will help in every way possible. But for securing those particular sites in this way, it is a DOD equity.

Mr. PFLUGER. Mr. Jones, for the border, I was down in the RGV last year, and they told me that they had over 20,000 incidents just in a quarter of drones that were being operated by cartels. What's the danger along the Southern Border to our citizens, the safety of our citizens from drones?

Mr. JONES. Thank you, Chairman.

So you touched on the volume. The volume of activity within the 500 yards of our contiguous border on the south and even on the north is staggering. We have deployed detection technology. You mentioned 20,000. The significant threat is counter-surveillance. They are surveilling law enforcement activities. They're doing this 24/7, 365. You know, historically we've had to—they've had to have high ground or terrain. Now, everywhere is the high ground. They have a tactical advantage.

Mr. PFLUGER. So they can see what's going on?

Mr. JONES. Exactly.

Mr. PFLUGER. Do you have the authority to mitigate those physically or by other means?

Mr. JONES. So the Secretary has designated certain areas along our border as covered facilities, so, yes, the capability exists and the authority exists in those covered areas.

Mr. PFLUGER. Have those types of mitigations taken place?

Mr. JONES. Yes.

Mr. PFLUGER. Are we actively mitigating?

Mr. JONES. We are actively mitigating, yes, sir.

Mr. PFLUGER. How many—my time has expired, but how many events are we experiencing per year on the Southern Border?

Mr. JONES. So, for example, last year if we look at 45,000 detections on the Southwest, of those, 2,500, plus or minus, actually made an incursion. So now we're talking about a very small subset. A lot of the surveillance is taking outside of our jurisdiction in foreign air space. That makes it particularly challenging for mitigation.

Mr. PFLUGER. I bet we'll get back to these. My time has expired.

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

Mr. MAGAZINER. Thank you.

You know, I'll pick up on this same line of questioning. When a number of us visited the Southern Border last year, we heard from your officers about the challenges that drones were posing. One question I have is I understand they're being used primarily by the cartels for surveillance, you know, to see where your officers are so they can, you know, more effectively traffic people, narcotics, firearms, et cetera, across the border.

Do you see any evidence of the cartels using drones to actually move some of that contraband? Like I'm thinking specifically of fentanyl. Are they using UAS to actually move fentanyl across the border?

Mr. JONES. We have yet to see fentanyl being moved via UAS. We have seen other narcotics, albeit in small quantities. From a cost model, it's not as effective for cartels because the payload capacity is so small they have to make multiple trips. We have seen cocaine. We have seen heroin. We have seen methamphetamine. We've seen weapons. So there is a threat of moving contraband across our borders.

Mr. MAGAZINER. So the numbers, of course, are staggering. I think at one point in your written testimony you alluded to periods of as many as a thousand detections a week, but the number of mitigations at the Southern Border was 86 in fiscal year 2023 and 60 in fiscal 2024. So why so few as a percentage of the whole? What are the barriers that you're facing?

Mr. JONES. Well, again, many of these detections occur in foreign air space. Thereby, we cannot mitigate. Actually a very small percentage actually incur into the United States. So, for example, on the Southwest Border, only 5 percent of that large number actually effect an incursion. Of that we have very strict criteria, and they met the criteria. So the 60 that we mitigated in fiscal year 2024 actually met the criteria for mitigation.

Mr. MAGAZINER. So I'm going to ask about both the 5 percent and the 95 percent then. So the 5 percent that do come into our air space, is the criteria too narrow, you know, to bring them down? Why again so few?

Mr. JONES. Well, again, one of the things that's notable here is that those are not 2,500 unique identifiers. You have repeat offenders. So we take down or mitigate one drone of that large number, that could be responsible for hundreds of detections across the border.

Mr. MAGAZINER. I see. So these are events, not necessarily individual drones, these statistics?

Mr. JONES. That's correct.

Mr. MAGAZINER. OK. So on the 95 percent—or really, I guess, the 100 percent, even if you don't have the authority to bring them down, those that are over foreign air space, do you still have the ability, the technological ability to track where the operators are and to alert Mexican or Canadian authorities as to where the operators are? Can you explain what that process is like?

Mr. JONES. Absolutely. We do communicate directly with our foreign partners, and our communication is healthy. Our sharing of information is healthy. So what you just described is exactly what we do.

Mr. MAGAZINER. Is it working? Does it happen? I mean, when you notify Mexican authorities, for example, that, hey, we've got a drone and we know where the operator is, I mean, are they pursuing the operators? Do you have success stories? Again, are there gaps that need to be filled in that process? Can you elaborate?

Mr. JONES. Again, we have to rely on our—so in the case of the government of Mexico, we have to rely on our Mexican partners to respond. A lot of times these are in areas that are not highly populated. They're very difficult to get to. They're also controlled by cartels. So by the time law enforcement responds, it's very challenging for them. It's not from lack of effort or lack of communication. It's just a very difficult environment.

Mr. MAGAZINER. With the minute that I have left, I'll shift to Mr. Wiegmann.

On the issue of special events, of SEAR events, can you just elaborate a little bit more about why it is so important that the State and locals have expanded authorities? What should the appropriate guardrails be, you know, for those expanded authorities?

Mr. WIEGMANN. Yes. Each year the FBI can cover a number of special events, and DHS covers some as well. So we're talking about big events, like the Super Bowl, the World Series, the Indianapolis 500, that sort of thing. But, obviously, those are not the only events that could be subject to an attack or a drone threat.

You have many other football games, baseball games, soccer games, the World Cup, if you add them all up, just folks on sporting events, even forgetting about *New York Times* New Year's celebration, there's all manner of events, so we can only cover a tiny fraction of those in any given year.

So if Congress gives the authority to State and locals to engage in the same activity, that vastly expands the scope of what counter-drone protection could be identified.

Mr. MAGAZINER. I'll just note for the record—thank you—I understand the need to expand that authority for the State and locals for these special events.

Mr. WIEGMANN. Yes.

Mr. MAGAZINER. I will just highlight, though, I think training is going to be very important in this because there are plenty of people who fly drones at, you know, high school football games and stuff for legitimate reasons. We'll just need to make sure that the State and locals have the training to know how to kind-of go after the bad guys without overly penalizing the good guys, but I take your broader point.

I yield back.

Mr. WIEGMANN. Absolutely. That's a big part of it, the training.

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

The Chair now recognizes the gentleman from Florida, Mr. Gimenez.

Mr. GIMENEZ. Thank you, Mr. Chairman.

I know that we face significant threats now from the technology that we have right now, but right around the corner, if not already here, is AI. So some of the techniques that we use to mitigate current drones won't work on AI because they won't be piloted. They'll just be given a mission. They'll be given parameters of what to hit, and they'll hit it by themselves. They don't need to be piloted.

Do we have any capabilities to actually go kinetic, actually knock these things down either through, you know, some kind of a projectile or with high energy that fries the systems? Do we have any of that available anywhere?

Mr. JONES. Thank you for the question.

So without tipping our hand to our adversaries, I think it would probably be best and we look forward to providing you detailed briefing on our capabilities, kind-of where our heads are at, and we share your concern.

Mr. GIMENEZ. Yes, because I think that that not only concerns me as far as Customs and Border Protection and our personnel but also airports, large events, et cetera, where these drones can be used for really destructive purposes, so I'm really, really worried about that.

Mr. Jones, you said that you had legal authority to disable, to mitigate drones in certain areas. We have about a 2,000-mile-long border. So those areas, how many miles of the 2,000 do you actually have the authority to mitigate these drones?

Mr. JONES. Chairman, again, we're starting to get into an area I'm not comfortable with in an open forum, but we'd love to talk those details with you behind closed doors.

Mr. GIMENEZ. I take that to mean there's not too many miles, OK. So that's fair enough.

Have you seen any kind of—we know that the cartels, especially the Mexican cartels, are working with the CCP, the Chinese Communist Party. The CCP provides the chemicals to the cartels who then produce the fentanyl that's killing thousands of Americans every single year.

Do you see any link between—we see that link. Do we see any links between the CCP, China, and the drones, the technology that's being used to surveil our border and that's being used to help the cartels in their quest to transport people, drugs, guns, everything into the United States?

Mr. JONES. It's no secret that the preponderance of the UAS technology is manufactured in China and that the cartels are using

that very technology. We share your concerns. There's a reason why we don't use Chinese drones and whether they knowingly or unknowingly are potentially collecting information for the government of China.

Mr. GIMENEZ. That's it. That's all the questions I have. Thank you.

I yield back.

Mr. PFLUGER. The gentleman yields.

The Chair recognizes Mr. Thanedar for his questioning.

Mr. THANEDAR. Thank you, Chair Pfluger.

The operation of C–UAS technologies to intercept drones is sensitive as it generally requires seizure of property without a warrant. To do so, C–UAS technology operators must hack into the signal used to control the drones, which often involves hacking into the operator's cell phone or computer. As such, Congress has waived certain wiretapping and other privacy protections for agencies to carry out these activities.

As DHS and DOJ have began to operate C–UAS technologies, what have your agencies done to formally enshrine protections for privacy and civil liberties, any one of you?

Mr. WHEELER. Sir, I can speak for the way that the FBI conducts the mission.

We're very sensitive to those concerns. The information that is captured electronically from the technology that we use is just the information that has to do with the control of the drone, the flight, the telemetry data, if you will. Even if it is from—if it is being operated by a personal device like a cell phone, for example, the technology that we use does not capture any other information from there, and we're very sensitive to how that is collected.

Whatever that information that we collect, we don't maintain it if it's not a threat, if it is not part of a case. If it is part of something that we investigate, then our regular guidelines of legal process and how we would maintain evidence apply. But we're very sensitive to privacy concerns and making sure we get it right and do it correctly.

Mr. THANEDAR. All right. Thank you so much.

Congress is currently considering authorizing a pilot program for State, local, Tribal, and territorial law enforcement agencies to operate C–UAS technologies. Expanding these authorities must be done carefully as doing so requires waiving wiretapping protections and other critical protections to protect privacy and civil liberties.

How can we ensure the operation of such technologies potentially by a large number of law enforcement agencies will be closely coordinated with and overseen by Federal authorities?

Mr. Wiegmann, most critically, how can we protect privacy and civil liberties?

Mr. WIEGMANN. Thank you for the question.

So if the pilot program, the State and local pilot program you mentioned is adopted, there would have to be—the law would require training for all State and local officials. It would also require them to follow the same procedures that my FBI colleague just mentioned in terms of the type of technology they can use, type of data that they can collect, the rules of engagement, what type of

facilities they can craft so they can do it safely and would have to work with the FAA.

All of their activities would have to be approved by DHS and the Department of Justice working with FAA. So it's quite a labor-intensive process that we're envisioning under the State and local pilot program to basically get State and local authorities up and running so that they can mirror and do the same things that we do at the Federal level, and that includes privacy and civil liberties.

Mr. THANEDAR. Thank you. Thank you so much.

I yield back.

Mr. PFLUGER. The gentleman yields.

The Chair now recognizes the gentleman from North Carolina, Mr. Bishop.

Mr. BISHOP. Thank you, Mr. Chairman.

Is it—how do I pronounce your name? Is it "Wiegmann" or is it "Wigmann"?

Mr. WIEGMANN. It's "Wigmann."

Mr. BISHOP. Mr. Wiegmann, I want to bore into this just a little bit more. Some of the questions have indicated and then the answers indicate that you've got to be careful about revealing specific technological things. But I noted one thing when you were testifying you said the reason that you need expanded authorities—I believe I got this right—is that the effect of technologies to deal with this could violate laws on intercepting aircraft in flight and intercepting transmissions.

Did I get that correct?

Mr. WIEGMANN. That's right.

Mr. BISHOP. Maybe you can just help me understand a little bit better. If you've got like a mass spectator event, which is one thing that's been raised, it seems to me—how do you have like a—and you've also said—several of you have made the point that, you know, how you intercept data to prevent intruding on privacy and certainly certain types of data. I must tell you that has a sophistication level I don't really understand.

Why not just have a rule that anybody who flies a drone near a mass spectator event the drone is going to be destroyed in the air? Is that something that it would be hard to do? Then why do you need to intercept data in order to do that? If the object is there, destroy it.

Mr. WIEGMANN. So it's a good question. I think the way it works, as I understand it—and my colleagues can talk about this operationally—if you had, let's say, a football game and you would have a perimeter, it would be declared as a temporary flight restricted area.

Mr. BISHOP. OK.

Mr. WIEGMANN. So around that you are going to have a buffer zone. You have an area where it's a no-go, and then you have a larger area around that where you might want to detect what's flying, and then you have a larger area around that where you might be tracking, but, you know, regular commercial drone use is OK.

So as they're getting closer and closer to the facility, you're detecting originally the signals to see what is that drone. You're trying to identify a drone. Oh, is that——

Mr. BISHOP. Kind-of like a long-distance radar or something like that?

Mr. WIEGMANN. Exactly. So is that a UPS drone that's just delivering a package somewhere? Let it go on its way. If it's getting closer, right into the zone where you're just going to have to do something against it, so it's kind-of a calibrated thing. As you get closer and closer, then that's where you take the opportunity to use the technology to jam it, most frequently, rather than destroy the drone. You're interfering with its navigation in a way that confuses it and requires it to land.

That's what they do in these scenarios is to make it land somewhere rather than, like, it's not the same as, like, shooting it out of the sky is my understanding how it works. You're instead using electronic things to bring it down. So that's essentially how it works.

Mr. BISHOP. Is the technology—and I've always been curious about that. The first time I asked it in a hearing a couple of years ago, there was a, you know, twitter of laughter throughout the room about the naivete of thinking you could destroy the thing in the air. I guess maybe if it leaves debris to fall or something, I could understand that.

Mr. WIEGMANN. It could be dangerous also, I think. If you were just to, like, kinetically destroy it, I imagine there would be some hazards with that.

Mr. BISHOP. Should the average person looking at this or the average Congressman trying to understand it believe that these technologies where you can use electronics to force the device to land are successful or have a high degree of reliability? Maybe I'll direct that to Mr. Jones.

Mr. WIEGMANN. Yes.

Mr. JONES. So there's also nondestructive kinetic capabilities. So one thing from a law enforcement perspective we have to remember is if we can capture a drone, there's a forensic capability that allows us to glean information.

Mr. BISHOP. Yes.

Mr. JONES. So that's important to us, as well as avoiding or minimizing any collateral damage. We have to be very careful in any application of force in public areas. Responsible law enforcement, first do no harm.

Mr. BISHOP. Is any witness, you know, able to testify—because what you've essentially laid out is we've had a series of short-term reauthorizations of the authorities that now exist, and the issue is you want to expand the authorities.

I have concerns, especially after a variety of ways in which I think Government authority has misused power to intercept information or learn information about the American people and has gone too far, what are the—can anybody describe what the hesitancy is and why they're not significant or why they should be overruled and proceed with this more expanded authority?

Mr. Wiegmann.

Mr. WIEGMANN. Hesitancy in adopting the expanded authority or——

Mr. BISHOP. Yes, yes.

Mr. WIEGMANN. That's kind-of hard for us to answer because we support expanding the authority.

Mr. BISHOP. I understand.

Mr. WIEGMANN. But I think that it's important to recognize when you talk about intercepting signals, and so forth, as I mentioned in my opening statement, as Assistant Director Wheeler just mentioned, the types of signals that we're getting are the same types of information that is actually required to be broadcast and that anyone can pick up with a drone today. That's the FAA's rule.

So we're not talking—there is, I guess, a privacy interest, but it's the same type of information that we're now requiring—and it's a new regulation, but requiring drones to broadcast so that anyone can pick up, because it's really just about the communications between the drone and the controller so that we can figure out where is that person, what's the registration, what's the model, how do we deal with it? So I think the privacy interest is limited.

Mr. BISHOP. My time has expired. Thank you very much.

I yield back.

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

The Chair now recognizes the gentleman from California, Mr. Correa.

Mr. CORREA. Thank you, Mr. Chair.

I want to thank the witnesses for being here today, very timely issue for all of us I think. Your testimony and the questions show a little bit of a tension here between private property, private rights, but I think the bigger one here is protecting public safety.

A couple of times back home I had the chance to see some drones flying over my house looking in my backyard, frustrating, angry, didn't have any kinetic weapons with me, so they came and went. But on a serious note, I'm home to Disneyland. Worldwide it's still viewed as an American private enterprise symbol. I've got the Anaheim Ducks Arena, Ocvibe, that's being built right now, the Anaheim Ducks, SoFi Stadium nearby, World Soccer Cup coming to our area very soon, Olympics coming soon, so a target-rich environment, so to speak.

What you're saying, Mr. Wiegmann, specifically you said that the Federal Government does not have the bandwidth to really protect all of these sites, yet we're still not at a point where we can share the authority information with State, local, Federal authorities. I hope we don't have to wait for a Federal law to be passed to get there.

My local sheriff in Orange County has a fusion center. Fusion centers exist across the Nation where Federal, State, local, FBI, every agency collaborate, share information, because when it comes to these drones, time is of the essence. Authority to neutralize these things is of the essence.

I guess my question to each and every one of you, starting with Mr. Jones, do you know of any efforts right now to coordinate with our locals to begin sharing, creating the local authority to be more effective at protecting our citizens?

Mr. Jones.

Mr. JONES. I would like to speak broadly and just—outside of just counting UAS, we are working with our Federal, State, and local partners on a daily basis. There is counter-fentanyl, counter-

UAS, just general public safety. They're our partners. We're all on the same team. We need the authority——

Mr. CORREA. I'm glad to hear you say that. Go ahead.

Mr. JONES. We need the authority to designate select State and local law enforcement, and then with approved equipment, you know, just like my colleague stated——

Mr. CORREA. We need a Federal law.

Mr. JONES. Yes, we do.

Mr. CORREA. Some of us here could probably do something like that, Mr. Chairman.

I hope we can also—I didn't hear it, I know, Mr. Gimenez's question talked a little bit about Mexico cooperation. Any there? This is something that deals with both sides of the border.

Mr. JONES. Like I stated earlier, our relationship and our information sharing with Mexico is healthy, both at the local level through the U.S. Border Patrol Foreign Operations Branches, as well as our communications with Mexico City.

Mr. CORREA. Thank you very much.

Mr. Wheeler, the same question to you. Do you know of any efforts to coordinate past laws to help us work with the locals to protect our citizenry?

Mr. WHEELER. Sure. I would illustrate as maybe a good example for the situation in New Jersey and our Newark division we talked about earlier, the FBI Newark JTTF, comprised of a lot of State and local officers that work on the JTTF, are our people that are actively investigating this matter.

Mr. CORREA. Are there any efforts to pass legislation that you're aware of to give the locals the authority to neutralize/monitor these aerial vehicles?

Mr. WHEELER. Well, that's not my purview to—for the legislation, but I can tell you——

Mr. CORREA. That you're aware of.

Mr. WHEELER [continuing]. I support capacity building for our State and local partners.

Mr. CORREA. Mr. Wiegmann, my last 30 seconds.

Mr. WIEGMANN. That's what we're here for, Congressman. There's a Senate bill. There's a couple of House bills. All of them——

Mr. CORREA. Good.

Mr. WIEGMANN [continuing]. To different degrees would provide additional authority to the States, both at a minimum to do detection only and then, on a pilot program, to do mitigation as well. So that's——

Mr. CORREA. Beyond those bills, do you see any—beyond those bills, any other authorities that are needed to be vested in the locals to do their job?

Mr. WIEGMANN. I think those bills are where we should focus in coming up with something that will work.

Mr. CORREA. Thank you very much, Mr. Chairman. I'm out of time. I yield.

Mr. PFLUGER. The gentleman's time is expired.

The Chair now recognizes the gentleman from Louisiana, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman.

Gentlemen, thank you for being here today.

It's been referenced that there are Federal laws against intercepting aircraft or intercepting communication signals, and it's been cited today regarding the absence of a specific Federal law authorizing local law enforcement to use existing technologies to mitigate against an unmanned aerial system threat or a drone threat.

Let me say that, Mr. Chairman, I believe that the Tenth Amendment already extends such rights to the sovereign States.

Let me say that the current law, the current Federal law that authorizes specific Federal law enforcement agencies to use existing and emerging technologies to mitigate against unmanned aerial systems, yes, that authorizes those specific Federal agencies to deploy that technology, but in no way does the current law prohibit the rights of the sovereign State to authorize their own State and local law enforcement to use existing technologies and emerging technologies in a law enforcement capacity.

Mr. Wiegmann, is it against the law for one American to strike another American? Yes, it is. It's not a trick question. Is that against the law?

Mr. WIEGMANN. You know, obviously, it depends on the context.

Mr. HIGGINS. Of course. There's a general law against that.

Mr. WIEGMANN. Yes.

Mr. HIGGINS. Is it allowed for a law enforcement officer who has probable cause to detain you or arrest you, is it allowed for him to strike you in order to effect that arrest? Yes, of course, he can.

Is there a law against me crashing my car into yours purposefully? Yes, there is.

But, Mr. Jones, are you familiar with the PIT maneuver? Of course. Law enforcement have been using this for decades. We use our vehicle to crash into a suspect's vehicle in a particular manner reflective of our training in order to effect the arrest.

We're using the current training standards and the technology of our vehicle that we have deployed to effect that arrest. That's not a vehicle crash, it's a law enforcement action.

It's broadly known, everyone knows it's against the law for one American to shoot another one; but a law enforcement officer, in order to effect arrest, if he needs to escalate to lethal force, we know a law enforcement officer has that authorization through Federal and State law.

So yes, there's plenty of laws. You guys love to cite these laws that exist that we cannot intercept an aircraft. We understand that. But if intercepting the aircraft is a law enforcement action which using existing technology to mitigate against an unmanned aerial threat, Mr. Chairman, these technologies exist.

Absolutely, our local and State law enforcement entities should have access to the same technologies that we seem to be very protectively reserving for only select Federal agencies.

So, Mr. Jones, you had stated earlier, good sir—and thank you for wearing the badge, my brother. You had stated earlier that, yes, you're deploying these systems.

But please clarify for America that there are great restrictions on actually deploying the technology to land a drone. You're using the technology primarily to track criminal drones, but you're not using

that technology primarily to land drones, which is what the technology does.

Am I correct in that assessment or not, Mr. Jones?

Mr. JONES. Well, both are true. We are using technology to track the drones. We are also using technology and electronic means to intercept and land the drone at a place of our discretion.

Mr. HIGGINS. Give us the numbers by percentage. If you track 100 drones, how many are you landing?

Mr. JONES. Well, like I stated earlier, for fiscal year 2024, Southwest Border, we actually landed 60 of them, mitigated 60 of those aircraft.

Mr. HIGGINS. Sixty of the 45,000 that you encountered? Well, there you go. That's what I'm saying. You're using the technology to track, but you're not using the technology to fully mitigate.

So this is what we've been talking about for a year, Mr. Chairman. This technology, by Tenth Amendment right, belongs to the sovereign States, and they should be allowed to fully deploy it.

Thank you, Mr. Chairman. I yield.

Mr. PFLUGER. The gentleman's time is expired.

The Chair recognizes the gentleman from Texas, Mr. Gonzales.

Mr. GONZALES. Thank you, Chairman.

You know, sometimes I feel like I'm in The Twilight Zone up here. Like month after month people come before us, they testify, and you don't get a lot of answers. It's concerning. It's frustrating.

You're telling me we don't know what the hell these drones are—in New Jersey are? Is that correct?

Mr. WHEELER. That's right.

Mr. GONZALES. That's crazy. I mean, that's crazy. That's madness that we don't know what these drones are. You're telling me that a lot of these—Mr. Jones, you're telling me that 90 percent—95 percent of these drones along the U.S.-Mexico border we can't interact because they're not in U.S. territory?

Mr. JONES. That is correct. A large proportion of them stay in foreign air space.

Mr. GONZALES. I'll tell you what, there are a lot of Americans that are very frustrated right now that are essentially questioning, Where are my taxpayer dollars going? You know, this DOGE craze that's kind-of starting to take hold. This is very real. I mean, this is going to come.

People are going to have to come before the carpet and they're going to have to explain every single line item. What do you do here? What does this get?

So, let me ask a very specific question. Mr. Wheeler, how much of the FBI budget goes toward counter-UAS?

Mr. WHEELER. So the technical part of operational budget that I have within the Critical Incident Response Group is less than $500,000.

Mr. GONZALES. Five hundred thousand dollars? That's nothing. Why is it so low?

Mr. WHEELER. Well——

Mr. GONZALES. No wonder we don't know what the hell is going on, $500,000.

Mr. WHEELER. So that number doesn't capture the—like the FBI Newark investigation, for example. That—the budget allocation for

what we're doing investigatively is not captured in that number. But for the technology we use and the way we deploy it, just under $500,000.

Mr. GONZALES. We want to help you. I mean, this is a committee, we—you know, the Chairman is putting this together because we want to know those topics. The American people deserve to know the truth on this, and we also deserve to have actions on it. If it's a budget issue, no problem.

But it's also a, "what is our money getting us?" Clearly, not a whole lot. Something needs to change, though, and I'm trying to figure out what that something is. Just month after month, it's the same-old, same-old. From a CBP standpoint, Mr. Jones, do you know what the current budget of CBP is for counter-UAS?

Mr. JONES. I can tell you that direct appropriations for counter-UAS was zero last year.

Mr. GONZALES. Zero? So—yes.

Mr. JONES. CBP took it out of HIDTA, and we will continue to take it out of HIDTA. Now, I can't tell you exactly what that number is. I have a general ballpark. But we can discuss that. I'll provide that as a get-back to you.

Mr. GONZALES. Another committee that I sit on is Appropriations, so I see a lot of things through the lens of dollars and cents. If you're putting zero on the board, you're probably not going to get a lot of success, and it's not fair.

You know, a lot of people talk about the border. I represent the border, nearly half of the Southern Border. I've been out there with these agents in the middle of nowhere that are essentially alone and unafraid, you know, making do with what they have.

It's not fair to them, and ultimately, it's not fair to us to have them combat against some of these drones that are happening with a zero budget. I mean, it's just madness.

So, you know, I guess—I have another line of questioning, but I don't want to embarrass anyone. I would just say I would be very interested in partnering up and figuring out what we need to do in order to find—answer some of these questions. What resources do you need?

The technology is already out there. Drones, this isn't new. Drones are 100 years old. This isn't state-of-the-art. I mean, drones are old technology. The fact that we don't know what's flying in our air space is only the tip of the iceberg what's to come.

We have to fix this, and I want to partner up to fix this. Part of that is finding out the proper resources you need, training, authorities. I get the authorities piece. But it's a cradle-to-grave type of situation. It cannot just be—the answer can't be we don't know and the answer can't be zero. I mean, we got to do better than that. If we don't, I suspect not-good things will happen.

So thank you, gentlemen, for coming before us and testifying. I look forward to partnering with all your agencies.

I yield back.

Mr. PFLUGER. The gentleman yields.

The Chair now recognizes the gentleman from New York, Mr. D'Esposito.

Mr. D'ESPOSITO. Thank you, Chairman.

I sort-of feel the same way as my good friend, Mr. Gonzales. This is like dèjá vu. We've been talking about this for a long time, and it seems to be not getting much answers.

I mean, the Chairman and I visited New York City probably close to 2 years ago. We met with the leadership in the NYPD. It was probably one of the most rapidly-growing drone use in the country. My vision on jurisdiction of taking down drones may be different from others here, but first, I think it's important to quickly focus on stuff back at home.

I mean, these drones over New York and New Jersey flying over critical infrastructure, flying over some of, whether it's the Verrazzano Bridge or others, I mean, I have to agree with my colleagues.

The fact that we continue to say that we don't know what they are, we don't know what they're doing, I mean, the American people are looking at us and they think that we are lying to them, because they think, How could you possibly not have answers to drones flying over some of the most critical air space in the country?

So, I mean, if we're expecting the American people to believe in the information that we're giving them, I think we do need to do better. That's none of your fault. I mean, the fact that there is only a, you know, half—what is it, a half a million dollars in drone expenditures, appropriations, that's absolutely insane and I hope that it's something that my colleagues work on.

But as many have already pointed out, drones continue to rapidly advance and become more readily available. Along with the expansion, threats from drones being used by bad actors have only increased, as all of you have mentioned. Right now, counter-UAS authorities are restricted from local law enforcement agencies, leaving it largely in the hands of Federal agencies.

So, Mr. Wiegmann or Mr. Wheeler, a very simple question: Do Federal agencies have the ability to assist local law enforcement agencies with their counter-UAS capabilities everywhere and every time it's needed?

Mr. WIEGMANN. Not today. That's what we're seeking from the Congress.

Mr. WHEELER. That is absolutely correct.

Mr. D'ESPOSITO. Are there events and places that would benefit from counter-UAS capabilities that Federal agencies are simply not able to cover?

Mr. WIEGMANN. Absolutely, there are.

Mr. WHEELER. Yes.

Mr. D'ESPOSITO. In your submitted statement, you both said, "We need to empower State, local, Tribal and territorial law enforcement agencies across the country, which are primarily responsible for keeping our citizens safe at the local level, to take the steps needed to protect their communities from the emerging threat."

This past year, right in my district, in the middle of my district in Nassau County, we hosted the 2024 International Cricket World Cup, including the India-Pakistan match. While there were drone-related threats from ISIS ahead of the tournament, the Federal

Government was only able to assist with their counter-UAS capabilities for a small portion of the tournament.

What is the current impact of local law enforcement not having these authorities? I'll leave that to any of you.

Mr. WHEELER. Well, I think that's the main thing is capacity. We need more capacity to be able to do the mission, and we strongly support State and local jurisdictions having that capacity and authority and ability to help.

Mr. D'ESPOSITO. Right. I think what's—I'm sorry, Mr. Wiegmann, I didn't mean to interrupt.

Mr. WIEGMANN. That's right. Just to answer your question also, Mr.—Congressman Gonzales, as well, I mean, I think all of us on the panel share your view that we need to do more and more resources. If we do get the authorities, we will certainly need more resources.

Even if State and locals are doing it, that will require training and additional work and approval on our end. So more resources, more authorities, those are all things that we would support.

Mr. D'ESPOSITO. I think it's important to point down and to spread the message, because I think there's a lot of false information being spread about law enforcement agencies trying to say that, well, they don't want this added enforcement. They don't want to take on this responsibility.

I mean, we had a hearing in this room just hours ago where the commissioner of the Nassau County Police Department, Patrick Ryder, was here. He has been advocating in his position as commissioner, as his position as a member of the Major City Chiefs, that this is something that local law enforcement agencies, not only do they need it, they want it.

I think that we have the opportunity throughout this country to make sure that law enforcement agencies, there is some sort of consolidation. There are many law enforcement agencies that border one another that could help each other deal with this, I'll call it a burden but this added burden, but they're willing to do it.

Why? Because it makes sure that people can be kept safe. We can make sure that in instances like the World Cup back in my district or as Mr. Gimenez was talking about, the Summer Games in Miami, I mean, to depend on the Federal Government and the Federal Government is telling us, Well, we can only help you some of the time, even when you have threats from ISIS, I mean, that's a huge problem and it's one that we need to address not only here today, but moving forward.

Mr. Chairman, my time is expired, but thank you for continuing to bring this to light.

Mr. PFLUGER. The gentleman's time is expired.

The Chair recognizes the gentleman from Arizona, Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman, for holding this hearing today.

Thank you, gentlemen, for coming today.

I got an article right here, "Mystery drones spotted over New York, New Jersey prompts calls for Federal investigation." I believe this was *Breitbart News.*

I want to start with you, Mr. Wheeler, from the FBI. What can you tell us about what you guys do know?

Mr. WHEELER. So the public reports and what we have from eyewitness sightings, some of those very credible police personnel and others, are what we describe as unidentified drones.

We do not know the particular specifics of what those drones are. Some are described as being slightly larger than a commercial available drone, fixed wing as well as rotary.

We have helped analyze with our partners' video and pictures of what those look-alikes would have been submitted. Part of that is these over 3,000 tips from the public and to look at that. But as I briefly stated, we don't know the people responsible behind that, and that's what we're working on——

Mr. CRANE. Yes. What did you say you guys were the FBI was spending on counter-drone?

Mr. WHEELER. My budget that would specifically include; the technology that we use.

Mr. CRANE. Was it $500,000?

Mr. WHEELER. Five hundred thousand dollars.

Mr. CRANE. That doesn't seem nearly adequate. Why do you feel like there isn't a push within the FBI to keep up with modern warfare and modern threats?

Mr. WHEELER. So we're——

Mr. CRANE. What is the budget for the FBI right now?

Mr. WHEELER. Roughly $11 billion.

Mr. CRANE. OK. Why do you think as warfare changes, and as you know, sir, warfare is changing drastically right now overseas especially with Ukraine and Russia and the development of drone technology, why isn't the FBI taking this threat more seriously, and that's obviously reflected by the budget that you guys have assigned to counter-drone technology.

Mr. WHEELER. I have a limited capability that is embedded within our Emerging Threats Unit for surveillance issues. That allocation of resources, that research, that operational deployment of our capability is what we have today. I would imagine that this would grow over time.

Mr. CRANE. What do you think that some of these terrorist cells that might be in the country right now or maybe even outside of our borders what do you think that they're looking at when they see a hearing like this and they see that you guys still after almost a month don't know who these drones are what do you think that they're thinking?

Mr. WHEELER. So, I would be measured in how we speak about our capability, and what our limitations and capacity is. However I'll say to you that it's not as good as I wish it was, and we'll continue to work to make it better.

Mr. CRANE. Well, when you're only spending $500,000 a year, it's probably not going to be very good, is it?

Mr. WHEELER. The only thing I would say about that is that this is an enterprise-wide problem, it's not just a technological problem. That most of that $11 billion budget for the FBI gets after threats to Americans, this being one of them.

The way we apply resources, personnel, operational, all of that to include technology to get after a threat that would threaten American lives, I don't think that $500,000 for the technology part of it adequately captures our commitment to protecting Americans.

Mr. CRANE. I want to shift real quick because you guys have been talking about using electronic warfare to counter some of these drones.

What about drones that aren't susceptible to counter-warfare, like your fiber optic drones; what are you guys doing about those?

I'll start with you, Mr. Jones.

Mr. JONES. So all options are on the table right now. We are using—we are exploring kinetic options to complement the electronic.

Mr. CRANE. You know you can buy those right now and they're really not that expensive. Are you aware of that, Mr. Jones?

Mr. JONES. I'm aware there's a lot of different technologies out there. We have experimented with some that have been very successful.

Mr. CRANE. Thank you. I yield back.

Mr. PFLUGER. The gentleman yields.

The gentlelady from New York, Ms. Malliotakis, is recognized.

Ms. MALLIOTAKIS. Thank you, Chairman Pfluger.

Thank you all for being here today. I just want to follow-up on what my colleague asked regarding what happened in New York and New Jersey.

These drones, unmanned aircrafts have also flown over my district. A number of constituents have seen them over a power plant in Brooklyn. They were coming over the Verrazzano Bridge. I will remind everyone or explain to everyone here that Verrazzano Bridge connects Staten Island and Brooklyn, and on the Staten Island side, you have Fort Wadsworth, which is a U.S. Coast Guard Sector New York base.

Then in the Brooklyn side right on the other side of the Verrazzano Bridge, you have Fort Hamilton, which is a U.S. Army installation. So, it is very concerning to me that we have these objects. We are not sure if they're drones or unmanned aircrafts, but they are flying over sensitive infrastructure and facilities.

The fact that we don't know what they are or who's behind them or what they're doing is very concerning to me, particularly in a post-Chinese spy balloon world. OK.

The fact that this administration allowed for a Chinese spy balloon to go across the country over multiple military installations is very concerning. That we could potentially be having this happen again is—it's like astounding to me that this is even happening without any type of intervention.

You say it's no known threat, but is there still a possibility of there being a threat? At the end of the day, that's what my constituents want to know.

Mr. WHEELER. Yes. I am cognizant, and we all are in the FBI, of what the threat can look like, any way of across the spectrum of sophisticated state actors/adversaries that want to hurt us all the way through counterterrorism matters, cyber, WMD, criminal, all the way down to a nuisance drone that could cause harm. So that's the wide spectrum that concerns me every day.

Ms. MALLIOTAKIS. And—OK. Want to finish your sentence?

Mr. WHEELER. I'll just mention it concerns me that we don't know the answer to your question yet.

Ms. MALLIOTAKIS. Are you working with the Pentagon, with FAA, with DHS, with your partners to try to identify this? Because I don't put it all on just the FBI. I think this is—I mean, why is—what is Homeland Security doing? Do you have any idea? Have you——

Mr. WHEELER. I wouldn't speak for another department, but I will say that the way we do business is extremely collaborative in the interagency, and especially with our State and local partners.

Ms. MALLIOTAKIS. So who is taking the lead here on this particular issue, identify these drones and aircrafts?

Mr. WHEELER. Well, we have an investigation open predicated on the—an idea that there's unsafe operation in the air space, which is a Federal violation that we have some jurisdiction for.

But it would help us know sort-of what lane this falls in when we know the people that are responsible and what this is all about, to your point earlier. We're actively investigating and would like to answer those questions. I don't have a better answer.

Ms. MALLIOTAKIS. What if they were carrying chemical weapons or something? We just don't—I mean, this could be already—this could be a much worse conversation we could be having right now, because these things have been flying all over New York, New Jersey, over military installations.

I don't know. I think—I don't know what's going on there, but these agencies need to figure it out and try to get to the bottom of what's going on. I think it's very concerning.

Is there a possibility—if hopefully it is not a threat, is it a possibility it would fall under this System Assessment and Validation of Emergency Responders program, the SAVER program? This is a program under Department of Homeland Security Science and Technology, where they are testing various technology for search-and-rescue, disaster response, and it could be part of the law enforcement assessment. Do you think that's a possibility?

Because my Army base doesn't know about it. My NYPD doesn't know about it. So I guess my question is, why wouldn't the local authorities know if this was part of a testing of security technologies for first responders?

Mr. WHEELER. I don't know that to be the case, and I couldn't really comment on that.

Ms. MALLIOTAKIS. OK. Well, just again, I would love to speak to you off-line at some point and maybe share some information with you. But I would really just urge if you could speak to your colleagues and counterparts in these other departments and—because we need to get to the bottom of what's going on here.

If it is something that is not nefarious and is one of—part of these public safety applications that are being tested, they need to coordinate with the local authorities, so my guys in New York NYPD, they know that it's not a threat.

Mr. WHEELER. I would agree.

Ms. MALLIOTAKIS. Thank you.

Mr. PFLUGER. The gentlelady yields.

This will be the last questioning from—for the first panel. The Chair now recognizes the gentleman from New Jersey, Mr. Smith.

Mr. SMITH. Thank you so very much, Mr. Chairman—Chairmen, both of you, for allowing me to sit in on this hearing.

I've been in Congress 44 years, and I have lost track of the number of times when we seemingly did not adequately assess a threat. I had one of my service members from the Marines in the barracks in Lebanon when that terrible horrible deed was committed by Iran. I—actually, after we got hit in Dar es Salaam and Nairobi in 1998 by al-Qaeda, I chaired all the hearings.

We had the chairman of Joint Chiefs of Staff come and testify, as Admiral Crowe. They kept saying, everyone, no one thought that al-Qaeda would hit there. Maybe in the Middle East but not there.

I wrote a bill called the Embassy Security Act. It was signed into law. I added it to an appropriations bill, big thick bill. It was all about setbacks and Mylar on the windows, a lot of good things. It did mitigate I think some of the concerns there.

But we always seem to miss something, and I'm very concerned that we're missing something here. I've raised the issue as has my colleague, Malliotakis and others in New Jersey and New York, about these drone sightings.

So last night, I was on the beach in Island State Park in Ocean County with the sheriff. He's—he has been working every single night. He's got his own tethered drones chronicling.

One of his officers, 2 nights ago, saw 50 drones come in off the ocean right there. So he thought maybe they'll replicate it. They didn't, but we thought it was a possibility.

Then last night, we had a number of other people there, including a commanding officer from the Coast Guard, who said that 1 of their 47-foot motor lifeboats was followed by between 12 and 30 of these drones as they went through the water, followed right behind them, you know. I said, what's the rules of engagement? I mean, you do it if you're fighting against, you know, a narcotrafficker or something. They said, We don't know, we don't have any.

So I did reach out to the commanding officer at the Joint Base, which is also in my district, and talked to him, had a very good conversation. Colonel Anthony Smith, Joint Base Fort Dix-McGuire, the 87th Air Wing, Air Base Wing, today.

I said, I know you have the capability—you've put out press releases—to identify and bring down drones. Why can't you deploy them at least to the ocean, bring one of these down, find out who's doing it? They have the capability.

He said, we don't have the authority, only within the parameters of our base. Well, there's a national interest here. Our jets fly over the ocean all the time for training, so that perimeter is larger.

So I did write Secretary Lloyd Austin asking that that capability that may be sitting in a closet somewhere—I know they use it all the time—but, you know, bring it out. I'm not saying you got to share it with the sheriffs. It would be nice. Just do it yourself in the interests of the American public.

So I would ask if you would echo that request. I mean, DOD has got the capability. Maybe Homeland Security does as well. When we had a Zoom meeting with Secretary Mayorkas—our Governor put it together, and I appreciated that. But I asked him, Why can't we just track where they go to? Seemingly, they're going out to sea to something, a ship. We don't know for sure. But they came in off the—off the, you know, from the ocean.

So the question really is, can't we just get DOD to share? In my first term, DOD and VA did a great thing, the DOD–VA sharing agreement for health care capabilities. It was fantastic. Why can't the DOD share this with Homeland Security, with FBI and others so that you can go out and find out who they are?

Maybe it's China. I chair the China Commission. You know, I've had 115 hearings on it. I'm barred from going there now. China—and I'm on their hit list. Xi Jinping is a monster. You know, look what Putin is doing. They're all capable of doing horrible things to our people. Now they're threatening my good friend and colleague from New York and, of course, New Jersey big time.

So let's go get that DOD capability and find out and put to rest the question, Who is it? We can bring one down tomorrow. Your thoughts.

Mr. WHEELER. Sir, I'd just say, I share your concern. I share a lot of frustration. I'm more than willing to continue working with the Department of Defense to try to get better.

Mr. SMITH. Again, if they don't have the authority, they can do it on an emergency basis. Just send that capability out to the ocean or to the beach, because they're coming in every day. Figure out which one it is and bring them down, and then retrieve it and find out what's going on.

As my good friend, Malliotakis, Congresswoman Malliotakis said, you know, the thing with the balloon was mind-boggling, you know, over our bases, and we didn't see that that was a threat. Well, this I think is a very serious threat.

So, please, if you could get DOD to share that capability. Maybe Homeland has it. I don't know. Maybe you have it somewhere, but I know DOD has it. Thank you. Appreciate it.

Mr. PFLUGER. The gentleman's time is expired.

I thank the witnesses for your valuable testimony, for being here today, and for the Members and the questions.

We will now dismiss this first panel, take a brief 2- to 3-minute recess while we arrange for the second panel of witnesses.

[Recess.]

Mr. PFLUGER. The committee will come to order.

I am pleased to have the second distinguished panel of witnesses before us today on this very important topic, and I ask that our witnesses please rise and raise your right hand.

[Witnesses sworn.]

Mr. PFLUGER. Thank you. You may be seated.

Let the record reflect that the witnesses have answered in the affirmative.

I'd now like to formally introduce our second panel. Mr. Jeffrey Baumgartner serves as the vice president for national security and resilience at Berkshire Hathaway Energy; and Dr. Paul Schwennesen serves as the co-director of the Global Strategy Decisions Group, also my classmate from the United States Air Force Academy, class of 2000.

Thank you for being here.

We will now recognize Mr. Baumgartner for your opening statement of 5 minutes.

STATEMENT OF JEFFERY BAUMGARTNER, VICE PRESIDENT, NATIONAL SECURITY AND RESILIENCE, BERKSHIRE HATHAWAY ENERGY

Mr. BAUMGARTNER. Chairman, Ranking Members, and Members of the subcommittees, thank you for inviting me to testify. My name is Jeffrey Baumgartner, and I serve as the vice president of national security and resilience policy at Berkshire Hathaway Energy.

Today, I want to discuss how unmanned aerial systems threaten critical infrastructure. Berkshire Hathaway Energy businesses provide reliable, secure, low-cost energy to more than 13 million customers in the United States, Great Britain, and Canada.

Our commitment to our customers requires us to secure our infrastructure from all threats, including those posed by unmanned aerial systems. Critical infrastructure is the backbone of our economy and security, yet energy sector infrastructure and the transportation, communications, and water sector infrastructure we rely on face increasing threats from UAS, and the stakes for ensuring resilience and security could not be higher.

In recent years, UAS technology has become more accessible, affordable, and advanced. While these innovations offer immense potential, like enabling faster damage assessments of energy infrastructure, they also empower malicious actors.

Adversaries can use UAS to surveil facilities, deliver hazardous payloads, disrupt operations, and even conduct cyber intrusions. The Department of Homeland Security's 2025 Homeland Threat Assessment highlights UAS as a persistent and growing risk to critical infrastructure.

This warning isn't hypothetical. Last month, Federal agents arrested an individual planning to use a UAS to attack an electric substation. I hope we can proactively address the UAS threat before a significant incident occurs.

Despite the pervasiveness of the threat, existing Federal laws and regulations have not kept pace with the rapid proliferation of UAS technology.

Current frameworks primarily address safety and air space management, but lack robust provisions to counter malicious UAS activities. This leaves critical infrastructure companies vulnerable to increasingly sophisticated threats.

To address these risks, we must modernize our defenses while balancing the security measures with civil liberties. A comprehensive strategy that incorporates technology innovation, appropriate legal frameworks, and public-private collaboration, is essential.

I hope we can prioritize the following actions: No. 1, grant critical infrastructure companies limited authority to deploy advance detection and counter-UAS technologies. Investments in cutting-edge counter-UAS systems will ensure we can address current and emerging threats effectively.

No. 2, identify formal mechanisms for sharing actionable information about UAS threats and enable law enforcement at all levels with the tools and legal authorities to address UAS threats effectively.

The third is advanced research and development. Collaborative R&D will improve the ability to neutralize UAS threats without collateral damage.

The fourth and final, develop a comprehensive strategy to align regulatory, technological, and operational efforts at Federal, State, and local levels, while addressing privacy concerns and establishing clear legal parameters for UAS operations.

The private sector owns most of the critical infrastructure that provides key services, but protecting these assets is a collaborative effort. The National Security Memorandum on Critical Infrastructure Security and Resilience rightly emphasizes this partnership.

However, existing counter-UAS authorities for DHS and the Department of Justice are set to expire soon. Failing to renew and expand current authorities risks leaving critical infrastructure defenseless against the evolving UAS threat.

The window of opportunity to address these challenges is closing. By modernizing our defenses, updating our legal frameworks and fostering collaboration, we can safeguard critical infrastructure, protect public safety, and maintain our leadership in security and innovation.

We are ready to work alongside this committee, a coalition of critical infrastructure companies, and relevant stakeholders to effectively protect our critical services against the evolving UAS threat.

Thank you for holding this hearing and I look forward to your questions.

[The prepared statement of Mr. Baumgartner follows:]

PREPARED STATEMENT OF JEFFREY BAUMGARTNER

DECEMBER 10, 2024

Chairman Pfluger, Chairman Gimenez, Ranking Member Magaziner, Ranking Member Thanedar, and Members of both subcommittees, thank you for the opportunity to testify. My name is Jeffrey Baumgartner, and I am vice president of national security and resilience policy at Berkshire Hathaway Energy. Berkshire Hathaway Energy owns energy production facilities, utilities, natural gas pipelines and a liquid natural gas import, export, and storage facility. Our locally-managed businesses share a vision for a secure and sustainable energy future. Delivering low-cost, secure, and reliable energy service each day to more than 13 million customers and end-users throughout the United States, Great Britain, and Alberta, Canada, is at the core of everything we do. That is why we are committed to securing our energy services from all hazards, including unmanned aerial systems (UAS). I appreciate your invitation to discuss this important topic on behalf of Berkshire Hathaway Energy's businesses.

Critical infrastructure forms the backbone of our Nation's economy, security, and public health. These assets—including energy facilities, transportation hubs, communications networks, and water systems—are increasingly vulnerable to a wide range of threats from UAS. Berkshire Hathaway Energy's businesses have customers or energy infrastructure in 35 States, and our energy services enable our customers' way of life. Today, demand for electricity is growing dramatically across the economy to support evolving customer needs, as well as critical technologies like artificial intelligence and the proliferation of data centers that fuel our digital lives. Natural gas has grown to represent over 40 percent of electric generation as of 2023,[1] making protection of pipelines, compressor stations and related infrastructure particularly important. Providing secure, resilient, and low-cost energy services is a responsibility we take seriously so that our customers can thrive.

[1] U.S. Energy Information Administration, What is U.S. electricity generation by energy source? (February 2024), *https://www.eia.gov/tools/faqs/faq.php?id=427&t=3.*

THE EVOLVING THREAT LANDSCAPE

In recent years, the accessibility, affordability, and sophistication of UAS have surged. This technological proliferation has benefited a variety of industries with legitimate use-cases. We are hopeful that the Federal Aviation Administration (FAA) Part 108 rulemaking will advance our businesses' ability to fly UAS beyond visual line of sight (BVLOS) to enable faster damage assessments of energy infrastructure and restoration times for our customers and your constituents. Simultaneously, however, the ease of procuring cheap, sophisticated UAS has empowered malicious actors.

Adversaries can use UAS to:

1. Conduct Surveillance.—Equipped with cameras or sensors, UAS can collect sensitive information about critical infrastructure layouts and operations.

2. Deliver Payloads.—UAS can carry explosives, incendiary devices, or hazardous materials, posing a direct physical threat.

3. Disrupt Operations.—By interfering with air space near airports or power lines, UAS can cause significant disruptions.

4. Enable Cyber Intrusions.—UAS equipped with hacking tools can breach wireless networks and disrupt communications.

Incidents in the United States and around the world highlight the urgency of this issue. The U.S. Department of Homeland Security released its 2025 Homeland Threat Assessment in October. The annual assessment highlighted that the intelligence community "continue[s] to observe concerning UAS activity over sensitive critical infrastructure sites, which could interfere with regular facility operations, disrupt emergency response or authorized flight operations, and provide intelligence to malign actors."[2] The assessment raises instances where malicious actors have "considered using UAS to conduct intelligence collection, to drop explosives and other items on U.S. critical infrastructure for disruption purposes, and to endanger takeoffs and landings at airports via the mere presence of UAS."[3]

Critical infrastructure sectors—including energy, transportation, and communication—are particularly vulnerable. As the 2025 Homeland Threat Assessment highlighted, unauthorized UAS activities can disrupt operations, cause physical damage, and facilitate espionage. We have observed UAS flights over substations, pipeline compressors, and our liquid natural gas plant that may be providing intelligence for future attacks. The potential for UAS to carry hazardous payloads, such as explosives or conductive materials, further amplifies the risk to public safety and national security. For example, last month, Federal agents arrested an individual in Tennessee who planned to use a UAS to fly explosives into an electric substation. He was charged with attempting to use a weapon of mass destruction and attempting to destroy an energy facility.[4] When arrested, the individual was in the process of executing his planned attack, having armed the explosive device and powered up the UAS he intended to use.

PROACTIVE AUTHORITIES TO ADDRESS THE THREAT

Despite the clear and present dangers with UAS, existing Federal laws have not kept pace with the rapid advancement and proliferation of UAS technology. The FAA has established regulations for UAS operations, but these regulations primarily address safety and air space management and lack robust provisions for countering malicious UAS activities.

In pursuing the imperative to enhance counter-UAS capabilities, it is essential to balance security measures with the protection of civil liberties. Legislation must include safeguards to prevent abuse of authority and ensure that counter-UAS operations do not infringe upon individuals' rights to privacy and lawful UAS use. Implementing oversight mechanisms, transparency in operations, and clear accountability standards will help maintain public trust and uphold democratic principles.

While agencies like the FAA and the Department of Homeland Security (DHS) have made strides in regulating the use of UAS, significant gaps remain to fully address the threats:

---

[2] U.S. Department of Homeland Security, Homeland Threat Assessment 2025 (October 2024), *https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30'sep24-508.pdf*.

[3] Id.

[4] U.S. Department of Justice, Man Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and to Destroy an Energy Facility in Nashville (November 2024), *https://www.justice.gov/opa/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy-facility*.

1. Limited Detection Capabilities.—Critical infrastructure owners and operators lack legal access to the most effective tools to detect, identify, and track UAS.
2. Legal Constraints.—Existing laws restrict private sector and local authorities from deploying counter-UAS technologies, even for self-defense.
3. Coordination Challenges.—There is no standardized protocol for coordination among Federal, State, and local entities in response to UAS incidents.
4. Expiring Authority.—Existing counter-UAS authorities for DHS and the Department of Justice are set to expire later this month, threatening to leave a critical gap in the legal framework necessary to effectively detect and counter UAS threats in the public and private sectors.

REQUEST FROM CRITICAL INFRASTRUCTURE

To mitigate these threats, I propose the following actions:
1. Enhance Detection and Countermeasures.—Expand authorities for advanced detection technologies such as radar, radio frequency sensors, and AI-based tracking systems. Enable appropriate critical infrastructure owners and operators to work with law enforcement to deploy counter-UAS tools at high-risk sites with a limited authority that balances the need to address this pressing threat with respect for privacy and safety.
2. Strengthen Public-Private Partnerships.—Establish formal mechanisms for information sharing between the Government and private sector, ensuring timely dissemination of intelligence to prevent significant threats. Create incentives for infrastructure owners to adopt robust UAS security measures, and empower Federal, State, and local law enforcement agencies with the necessary tools and legal authority to address UAS threats within their jurisdictions.
3. Advance Research and Development.—Fund research and development programs focused on innovative UAS countermeasures and threat analysis. Promote joint exercises and simulations to test the resilience of critical infrastructure against both physical and cyber threats and the ability to neutralize threats without collateral damage.
4. Develop a Framework for Countering UAS Threats.—Direct DHS, in collaboration with the FAA and the Department of Defense, to lead the development of a comprehensive strategy that aligns regulatory, technological, and operational efforts to systematically address UAS risks. Establish a clear legal framework that defines the parameters for counter-UAS operations, including addressing privacy concerns, ensuring compliance with existing laws, and providing guidelines for the use of force in UAS mitigation efforts. Combine these efforts with appropriate State and Federal penalties for malicious use of UAS near protected facilities, including critical infrastructure.

CLOSING

The proliferation of UAS presents both opportunities and challenges. Critical infrastructure security is a shared responsibility and a national imperative. While most critical infrastructure is owned by the private sector, government at all levels can and must play a role in protecting this infrastructure, especially when there is a growing need to defend against nation-state actors. The U.S. Government has long recognized the private sector is on the front lines of critical infrastructure protection, as recently embodied in National Security Memorandum on Critical Infrastructure Security and Resilience.[5] To harness the benefits of this technology while mitigating its risks, Congress must prioritize the enactment of comprehensive counter-UAS legislation that enables an industry-Government partnership to address the evolving threat. By doing so, the United States can safeguard its critical infrastructure, protect public safety, and maintain its position as a leader in technological innovation and security.

The window of opportunity for Congress to address the escalating UAS threat is narrowing. With existing counter-UAS authorities set to expire and the rapid advancement of UAS technology, the time for action is now. Failure to enact comprehensive legislation will leave critical infrastructure vulnerable to malicious UAS activities, resulting in potentially devastating consequences for national security and public safety.

The threat of UAS to critical infrastructure is no longer theoretical—it is a reality demanding urgent and coordinated action. By modernizing our defenses, updating our legal frameworks, and fostering collaboration, we can ensure our infrastructure

[5] White House, National Security Memorandum on Critical Infrastructure Security and Resilience (April 2024), *https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/*.

remains secure against this evolving threat. I am hopeful that my testimony underscores the industry's commitment to security and our willingness to work with both public and private partners across all sectors to address all threats to U.S. energy security. Thank you again for holding this hearing.

Mr. PFLUGER. Thank you, Mr. Baumgartner.

The Chair now recognizes Dr. Paul Schwennesen for his opening statement.

STATEMENT OF PAUL SCHWENNESEN, CO-DIRECTOR, GLOBAL STRATEGY DECISIONS GROUP

Mr. SCHWENNESEN. Chairmen Pfluger and Gimenez, Ranking Members Magaziner and Thanedar, and distinguished Members of the subcommittee, thank you for the opportunity to testify today about safeguarding the homeland from unmanned aerial systems.

So I have rearranged my remarks, easily in the back, hoping to give you guys something a little more tangible to work with so that we're not just repeating and risking the constant repetition of the problem. I think we acknowledge the problem. We have a real train wreck coming.

I think it goes a little bit unsaid. I think we lack a lot of the technical know-how on how to deal with this, on how to assess and neutralize these threats. But there is somebody who does know, and that's the Ukrainians.

Having recently observed first-hand the astonishing evolution in drone operations in Ukrainian-occupied Kursk, I think the message for me, at least, has finally sunk home. Unmanned systems are not just an iteration. They are, indeed, a revolution in the application of lethal force.

The world's most advanced weapons and tactics are being developed and deployed at scale in the Ukraine Russian front at remarkably low-cost, and without central direction, and these facts hold radical implications for the next major shooting war between great powers.

We need to learn from the Ukrainians. The United States is rapidly losing its strategic military advantage in this new technical environment. There can be little doubt that China, North Korea, Iran, and other emergent powers are eagerly sending observers and technicians to the front lines in occupied Ukraine to very carefully note the revolution in weapons delivery and to adopt it into doctrines which seek to invert the military strengths of their larger, better-equipped, better-trained Western geopolitical adversaries.

We need to learn from Ukraine. In short, the rules of the arms race have been fundamentally rewritten to favor small, cheap, easily mastered weapon systems. More important still, these disproportionate advantages are not a one-time effect. They amplify in a positive feedback loop through each iteration cycle. New tech gets better exponentially faster and is deployed far more quickly than legacy countermeasures.

In Ukraine, the source of this immense innovation reservoir is the highly-adaptable, highly-diffused emerging engineering base of Ukrainian technicians. Uncountable tech workers routinely work full days in their civilian capacity, then leave their jobs to go work in pop-up tech facilities until late at night. The whole country is

on deck. They have created an ecosystem of invention, a web only loosely coordinated through the Ministry of Defense.

The advances in hardware and software they produce are channeled into a robust system of decentralized training facilities, and in less than 3 weeks, an FPV drone operator can be mission-ready. Operators with no previous battlefield experience have been credited with as many as 1,500 confirmed kills. The disproportionality is vast.

This is perhaps the main takeaway in a total-war, peer-to-peer scenario. If technology allows one side of a conflict to impose extraordinary damage on the exquisite, expensive, difficult-to-master weapon systems of their adversary, and can do so at a fraction of the cost expended by their enemy, it doesn't require an economist to see where that leads.

It is easy to be a critic, but I am convinced the United States and its NATO allies have a very narrow window of opportunity to address this major shift in comparative advantage. Current operations in Ukraine have shown what a scrappy, innovative force can do to a large, hidebound military machine. It would be well to take note.

So some of the scenarios looking forward: I think the most likely is that the United States will fall behind the leading edge of UAS development and deployment and will only start to respond in the aftermath of a crisis, and we're seeing some of that already in New Jersey.

We don't need a Pearl Harbor or a 9/11 to wake us up. We're already awake. We need to deal with this now. So the best case is possibly conceivably that we can avoid this kind of depressing scenario through a well-orchestrated demonstration.

Historical examples, such as the sinking of the Ostfriesland—Air Force people know this well—show that it is sometimes possible to break entrenched paradigms by publicly demonstrating the current system's vulnerabilities.

When understood by the right audiences, these demonstrations can shift doctrine development and tactical training in new and constructive ways, preferably before the lessons are learned the hard way.

We need to learn from Ukraine. It's time to get a task force to mop up information, go out there, sponge this stuff up, and learn from what they're doing and learn this information from in theater and get up to speed as soon as possible. Thank you.

[The prepared statement of Mr. Schwennesen follows:]

PREPARED STATEMENT OF PAUL SCHWENNESEN

THE 'DRONE WARS' IN UKRAINE—AND WHAT IT MEANS FOR AMERICA

Chairmen Pfluger and Gimenez, Ranking Members Magaziner and Thanedar, and distinguished Members of the subcommittees, thank you for the opportunity to testify today about safeguarding the homeland from unmanned aerial systems.

Almost exactly a year ago, a sniper team I helped convene engaged a Russian machine gun position near Bakhmut. While a handful of drones in the sector (both Russian and Ukrainian) encouraged a certain discretion on our part, they operated in a surveillance role only—while artillery and infantry assault forces fulfilled their traditional roles. One year later, such an operation would be effectively impossible—the hyper-advancements in weaponized drone technology would make such a comparatively exposed position untenable. The implications of this shift in tactical reali-

ties on U.S. and allied national security is only just beginning to dawn on the transatlantic defense establishment.

I confess it freely—I was a latecomer to recognize the enormous implications of drones (or "Uncrewed Autonomous Systems" if you must). I'd seen them deployed in Ukraine over nearly 3 years and felt (and wrote!) that while significant, drones represented merely an iteration in a manageable arms race. Like Stacie Pettyjohn and others, I felt that the hype risked overstating the case. Having once again observed first-hand the astonishing evolution in operations in Ukrainian-occupied Kursk, however, I think the message has finally sunk home: unmanned systems are not just an iteration, they are indeed a revolution in the application of lethal force.

The United States defense establishment does not appear equipped, technically or psychologically, to respond to this looming threat. I must emphasize—in the starkest terms—that the comparative advantage in modern weaponry has fundamentally and perhaps permanently shifted toward small, cheap, attritable, evolutionary systems. Expensive legacy weapons-systems, traditional procurement conventions, and standard training regimens are increasingly obsolete. The world's most advanced weapons and tactics are being developed and deployed (at scale) in the Ukraine-Russian front at remarkably low-cost and without central direction—and these facts hold radical implications for the next major shooting war between great powers.

The United States is rapidly and unwittingly losing its strategic military advantage in this new technical environment. There can be little doubt that China, North Korea, Iran, and other emergent powers are eagerly sending observers and technicians to the front lines in occupied Ukraine to carefully note the revolution in weapons delivery and to adopt it into doctrines which seek to invert the military strengths of their larger, better-equipped, better-trained Western geopolitical adversaries.

Technical advances, particularly in first-person view (FPV) drone deployment, mean that between 100 grams and 50 kilograms of high explosive can be delivered to within $50cm^2$ from 10km away, practically anywhere on earth, indefinitely and from every direction on the compass; flying through trees and terrain at high speed and inches off the ground. Rapid advances in navigation technology mean that the primary counter to drone deployment (frequency jamming) is increasingly irrelevant. Artificial-intelligence navigation modules that are capable of terrain navigating to their target are readily available. Small drones made of radar-transparent composites (even cardboard!) are likewise increasingly available, making drone interdiction an increasingly difficult prospect.

It is not just the technical advances that got my attention—the tactics of employment are equally striking. Ukrainians are, for instance, landing ambush drones on roads deep in enemy territory which can be activated to attack armored traffic when it appears. They use "carrier drones"—heavy-lift units that will carry 4 or more FPV drones into the battlespace to be deployed against multiple targets. They are using heavy drone decoys to draw anti-drone fire, then hit the source with smaller attack units. They have advanced laser-guided munitions being deployed at altitude. They are perfecting techniques to protect operators from counter-fire. They are dropping explosives, unseen and unheard from 5,000 feet directly into fighting holes by detecting body heat. There is no more "blending in with the terrain"—it is irrelevant. The cost of losing a drone is negligible and with zero loss of life.

In short, the rules of the arms race have been fundamentally rewritten to favor small, cheap, easily-mastered weapons systems. More important still, these disproportionate advantages are not a one-time effect—they amplify in a positive feedback loop through each iteration cycle. New tech gets better exponentially faster and is deployed far more quickly than legacy countermeasures.

In Ukraine, the source of this immense innovation reservoir is the highly-adaptable, highly-diffuse engineering base of Ukrainian technicians. Uncountable tech workers routinely work full days in their civilian capacity, then leave their jobs to work at pop-up tech facilities until late at night. They have created an ecosystem of invention, a web only loosely coordinated through the Ministry of Defense's newly-minted Unmanned Systems Service (an independent branch of the Ukrainian military). The advances in hardware and software they produce are channeled into a robust system of decentralized training facilities which operate on state-managed "polygon" ranges and private testing facilities. In less than 3 weeks, an FPV drone operator can be mission-ready: Operators with no previous battlefield experience have been credited with as many as 1,500 confirmed kills. Again, the disproportionality is vast.

And this is perhaps the main takeaway in a total-war, peer-to-peer scenario: such wars are heavily defined by economic considerations—the side that produces more materiel while absorbing material losses ultimately prevails. Training, esprit de

corps, fighting spirit—all are dependent on the products of a functional economy. Look no further than the Confederate States Army or the German Wehrmacht—their legendary fighting spirits ultimately collapsed under the sheer mass of the other side's more efficient war machine. If technology allows one side of a conflict to impose extraordinary damage on the exquisite, expensive, difficult-to-master weapons systems of their adversary, and can do so at a fraction of the cost expended by their enemy—well, it doesn't require an economist to see where that leads.

It is easy to be a critic, but I am convinced that the United States and its NATO allies have a very narrow window of opportunity to address this major and growing shift in comparative advantage. Current operations in Ukraine have shown what a scrappy, innovative force can do to a large, hidebound military machine—it would be well to take note.

SCENARIOS

Least Likely.—The U.S. Department of Defense will quickly integrate UAS technology and training from Ukraine into its mainstream, operational-level, front-line units. It would take an unprecedented level of commitment from all levels of the command structure and an extraordinary degree of political cooperation to shift the status quo.

Most Likely.—The United States will fall farther and farther behind the leading edge of UAS deployment and will only begin to respond in the aftermath of a crisis. My discussions with Capitol Hill legislators, front-line military leaders, defense analysts, and doctrine scholars lead invariably to the same independent conclusion: the American defense procurement system is too vast, and the regulatory frameworks too inscrutable, to meaningfully adopt UAS capabilities into existing defense doctrine or practice. An event akin to Pearl Harbor or 9/11, with the physical destruction of tens of billions of dollars of hardware and a substantial loss of life will be required to jumpstart the innovation cycle and break down the thickets of red tape which make initiative next to impossible.

Best Case.—Conceivably, this kind of depressing scenario can be avoided through a well-managed artificial crisis. Historical examples, such as the famous sinking of the Ostfriesland, show that it is sometimes possible to break entrenched paradigms by publicly demonstrating the current system's vulnerabilities. When understood by the right audiences, these demonstrations can shift doctrine development and tactical training in new and constructive ways—preferably before the lessons are learned the hard way.

Mr. PFLUGER. Thank you, Dr. Schwennesen.

The Chair will note that we had a third expert on the panel, Mrs. Cathy Lanier from the National Football League, unfortunately, unable to join today. However, the Chair asks unanimous consent to enter Ms. Lanier's testimony into the record. Without objection, so ordered.

[The prepared statement of Cathy Lanier follows:]

PREPARED STATEMENT OF CATHY L. LANIER, CHIEF OF SECURITY, NATIONAL FOOTBALL LEAGUE

DECEMBER 10, 2024

Chairman Pfluger, Chairman Gimenez, Ranking Member Magaziner, Ranking Member Thanedar, and Members of the subcommittees, thank you for the opportunity to testify today regarding the National Football League's efforts—in conjunction with several other sports organizations including NASCAR, Major League Baseball, and the NCAA—to address the significant and growing threats posed by unlawful drone activity in and around our games and other major events. Unlawful drone activity risks the safety and security of the tens of millions of fans and stadium-goers who attend major sporting events each year across the country.

I joined the National Football League in September 2016 after more than 26 years in local law enforcement in the District of Columbia. At the NFL, for the past 8 years, I have overseen the security policies and personnel that protect the 1,700 professional players, the hundreds of coaches and other staff associated with our 32 clubs, and the 17 million fans who attend our games each year. Club security officials and I work closely with local law enforcement officials, Federal authorities, stadium owners, and many others to provide a safe and secure environment for our fans to enjoy the games. In addition, I have served on the Homeland Security Advisory Council, and participated in the Department of Homeland Security's Critical

Infrastructure Partnership Advisory Council Working Groups. I also served on the Federal Aviation Administration's (FAA) UAS Detection and Mitigation Systems Aviation Rulemaking committee.

I last had the privilege of testifying in September 2018, before the Senate Committee on Homeland Security and Government Affairs when Congress was considering this same issue. Congress subsequently included the Preventing Emerging Threats Act in the FAA Reauthorization Act of 2018. That law took an important first step in protecting the homeland against rogue drones by providing counterdrone authority to Federal law enforcement officials at the Department of Justice and the Department of Homeland Security. Back then, and ever since, the NFL and other sports leagues have urged Congress to enact legislation that would take the appropriate next steps to meet this growing threat by providing counterdrone authority to State and local law enforcement officials, which are the entities that actually lead the work to provide safety and security at nearly all of our stadiums. They are at the front line providing on-the-ground protection to fans, players, and stadium and event officials. To be clear: We are not seeking mitigation authority for the NFL or other sports organizations. We seek that authority for the law enforcement partners with whom we work in ensuring a safe and secure environment for our events.

DRONE INCURSIONS ARE GROWING

In the 6 years since my earlier testimony, we have witnessed a sharp increase in the number of threats, incidents, and incursions by unauthorized drones, especially over the last 4 years. In 2022, we experienced 2,537 rogue drone flights into the restricted air space above stadiums during NFL games, and in 2023, the number of incursions grew to 2,845. To put these numbers in context, when I testified in 2018, we had tracked about a dozen incursions by drones at stadiums during games in the 2017 season. In the 2018 season, we tracked 67 drone incursions at games. Even accounting for the increased sophistication of our drone tracking abilities today, these statistics almost certainly understate the total number of events. Yet, even with that limitation, these statistics demonstrate the dramatic increase in drone incursions—rising by more than 20,000 percent between 2017 and 2023.

These incursions at NFL games included the following:

- In 2019, during the Super Bowl in Atlanta, an FBI team detected a drone in the restricted air space moments before 6 Air Force F–16s prepared to conduct a flyover before the game. Fortunately, the FBI team was able to communicate with the flyover team to prevent a collision.
- A Ravens vs. Bengals game was delayed in November 2023 because of a drone flying over the stadium bowl. After stadium authorities detected the drone, State law enforcement officials were notified and located the drone operator, who was interviewed by officials, including local FBI agents.
- In January 2024, the AFC championship game between the Ravens and the Chiefs was paused because a drone violated the restricted air space. Stadium authorities notified State law enforcement officials, who located the drone operator. The drone operator was questioned by State and Federal law enforcement and charged with 3 felony counts related to operating an unregistered drone, serving as an airman without a certificate, and violating national defense air space. The operator subsequently pled guilty to a misdemeanor.

Each and every one of these incursions violated long-standing law. Following the terrorist attacks of September 11, 2001, the FAA established flight restrictions over stadiums and other large gatherings. Congress subsequently strengthened and codified these requirements. The current version of the temporary flight restriction prohibits all aircraft operations over certain sporting events from 1 hour before until 1 hour after the event, from ground level to 3,000 feet, and within a radius of 3 nautical miles. In addition to NFL games, this flight restriction applies to Major League Baseball games, NCAA Division I football games, and NASCAR, Indy Car, and Champ Series races. The flight restrictions designate the air space as National Defense Airspace, and any operator who knowingly or willfully violates the flight restriction may be subject to criminal penalties.

This stadium and sporting event flight restriction is well-established and geographically and temporally limited. The FAA has a thorough and robust process for considering and approving waivers, which has effectively served the sports organizations, broadcast operators, and others for more than 2 decades. State and local law enforcement officials, however, still lack the authority to enforce the long-standing TFRs by taking action against rogue drones.

Our national security and intelligence agencies continue to warn that terrorist groups and other bad non-state actors consider stadiums and other mass gatherings

attractive targets for attack. In fact, earlier this year, Islamic State propaganda specifically encouraged attacks on stadiums, including referencing the Paris Summer Olympics. And social media posts recently threatened drone attacks at the Cricket World Cup on Long Island, New York.

H.R. 8610, THE COUNTER-UAS AUTHORITY SECURITY, SAFETY, AND REAUTHORIZATION ACT

Given the persistent threat, the NFL and other sports leagues have been leading proponents of legislation—the Safeguarding the Homeland from Threats Posed by Unmanned Aircraft Systems Act (S. 1631 and H.R. 4333)—that builds on the 2018 law and provides more robust and effective protections for the homeland in general, and major sporting events in particular. That bipartisan bill, which was first introduced in the previous Congress and reintroduced in this one, expands counterdrone authority to State and local law enforcement agencies through a 6-year pilot program, subject to Federal oversight.

In addition, we have appreciated the opportunity to work with senior leadership and staff of this committee, as well as the Transportation and Infrastructure and Judiciary Committees, to revise and improve H.R. 8610, the Counter-UAS Authority Security, Safety, and Reauthorization Act. We recognize the significance of the work, diligence, and cooperation of the committees to come together to introduce and mark up this bill in September.

The current version of H.R. 8610 is a step in the right direction. It would ensure that existing authorities for the Department of Justice and Department of Homeland Security do not expire, and it starts the process of empowering local law enforcement to keep fans safe. Nonetheless, we encourage the committee to make additional improvements to the legislation that gives sports leagues and our law enforcement partners the additional tools we need to better protect our fans.

We appreciate that the bill provides for a pilot program for State and local law enforcement counterdrone capabilities, and that the proposal explicitly includes stadiums in the definition of covered sites. As amended, the bill limits the pilot program to only 5 agencies, potentially expanding to 15, and further limits the program to just 4 covered sites per agency. First, we strongly recommend expanding the pilot program to adequately protect fans attending major sporting events. Specifically, we encourage the committee to increase the number of agencies and remove the cap on the number of sites that each agency could protect. These changes would better help us protect more fans in more places in a more expeditious time frame across the country.

Second, the regulatory process imposed by the bill is unnecessarily complicated and cumbersome, which will result in bureaucratic barriers that delay the deployment of counterdrone capabilities. Federal law already provides a proven framework for implementing counterdrone authority, approving technology, and selecting sites for protection, as outlined in the Preventing Emerging Threats Act and implemented by Federal agencies. The NFL supports maintaining this established framework, as proposed by S. 1631/H.R. 4333. In our view, there is no need to fix what already is working.

Third, we recommend that the provisions in the bill related to advanced drone detection technology, which is used to detect, track, and identify drones, be expanded to authorize deployment by critical infrastructure owners and operators, including trained stadium security personnel. Our stadium security personnel already have access to passive drone detection technology, and they should have direct access to and use of advanced drone detection technology, without needing to engage an intermediary. Detection technology has been used safely for years, and it does not present the more complicated legal issues associated with drone-mitigation authorities. Detection is not the same as disabling or "bringing down" a drone. That is a law enforcement function. By allowing private parties to use more sophisticated detection technology, we can better assist law enforcement partners.

CONGRESS SHOULD PRIORITIZE ENACTING COUNTERDRONE AUTHORITY FOR THE STADIUM TFR

Finally, we encourage the committee to consider prioritizing TFR-protected sporting events as a foundation for enacting any counterdrone legislation, and to do so as soon as possible. Given the growing threat of drones at stadiums and sporting events, and the long-standing and well-established flight restrictions over games and events, Congress should act now to extend counterdrone authority to State and local law enforcement agencies for the narrow, mission-specific, and time-limited purpose of protecting the sports stadium-TFRs when they are in effect.

We recognize that certain stakeholders have raised privacy and civil liberty concerns around counterdrone expansion—particularly when exercising counterdrone missions in certain circumstances or areas. Under current law, however, drones and other aircraft are simply not permitted in areas protected during a TFR. A drone operator flying a drone over a crowded stadium is already breaking the law. Therefore, we believe any privacy or civil liberty concerns are diminished significantly in the context of using proven counterdrone technology to enforce long-standing TFRs around sporting events.

Furthermore, Congress, the FAA, and national security agencies have made considerable strides in implementing a comprehensive regulatory structure for drone operations that lay the groundwork for immediately expanding counterdrone authority to State and local law enforcement to protect stadiums during live events. These steps included implementing Remote ID, adopting a comprehensive program for remote pilot certification, creating registration and labeling requirements for drones, and implementing Congress's modification of the hobbyist exemption, all of which the sports leagues supported.

Due to the Federal counterdrone authorities under current law, stadium operators and law enforcement now have a proven track record of safe, successful, and secure use of counterdrone capabilities at many NFL stadiums. As of today, Federal law enforcement authorities have safely and effectively provided counterdrone protections at 6 NFL stadiums that have hosted a Super Bowl. Technology, air space safety, and telecommunications questions have all been addressed at these stadiums, and we have a proven record of deploying counterdrone capabilities safely and effectively at these stadiums. The same technologies that have already been cleared for use in the National Airspace and safely deployed at these same stadiums should be permitted for use by State or local law enforcement to keep fans safe at games throughout the season.

The time to act to keep fans safe is now. Even in the waning days of the 118th Congress, we urge you to take any possible steps that will start to protect more of our fans from the threats of illicit drone use. Thank you for the opportunity to be here today, and I would be happy to address your questions.

Mr. PFLUGER. I now recognize myself for 5 minutes of questioning, as we did prior.

Dr. Schwennesen, I'd like to focus on something here. Policy versus technology, what is our issue right now? Is it not enough technology? Is it not keeping up with the technology—as you mentioned, maybe we're being outmaneuvered in a lot of cases by the Russians and the Ukrainians may have some information that we can learn from; or is it a policy issue here as we protect the homeland, or is it both?

Mr. SCHWENNESEN. I do think it's both. I think it's a combination of the two. I think we have created a policy thicket of bureaucracy that basically stifles the innovation space. I do think we have a technical know-how problem, or at least we can—or at least we know for a fact that Ukrainians have a technical know-how solution, right?

I think if we're able to reduce some of the—some of the bureaucratic barriers to innovation, allow people to tinker and experiment and learn at the operational military level, this needs to happen like yesterday, right?

We can't—we can't do the same old business of doing a 2½-year request for proposal and wait for things to come back. We just can't do this business as usual. We do not have that time.

Mr. PFLUGER. As we sit here, you listened to the testimony. We currently have UAS's flying over New Jersey. We heard from Mr. Smith in New Jersey that they were flying over Coast Guard vessels last night.

How is this possible? Why are we not responding? What do we need to do? What actions need to be taken?

Mr. SCHWENNESEN. That's a very difficult one to answer. Of course, I can't speak for them, but I have a suspicion that people are frozen with fear of what would happen in an administrative situation in which they took action and they were punished for doing so.

That they shot down a drone, God forbid, and the debris hit somebody's house, and all of a sudden they're on front-page news. So people are acting out of a sort-of sense of self-restraint here, which is being promoted by our policy environment.

Mr. PFLUGER. So when it comes to technology, we need to focus on our offensive technology, lessons learned in the Ukrainian conflict where they're leveraging UAS systems everywhere.

We need to focus on our counter-UAS technology, and our policy needs to improve in order to counter it, and then give the authorities that we need while protecting privacy of citizens here.

Mr. SCHWENNESEN. Yes. I would say so, absolutely.

Mr. PFLUGER. I'll come back to you in a second.

Mr. Baumgartner, what's the—what's the most catastrophic event in the energy industry critical infrastructure that we need to be thinking about and planning for to prevent?

Mr. BAUMGARTNER. I mean, luckily we haven't seen a significant incident. I think from an imagination perspective, certainly something with a payload, like the gentleman from Tennessee who was planning an incident to drop a payload into a substation.

You could imagine that at larger scale and impacting or identifying more critical infrastructure from generations of substations, or even on the pipeline side a liquid natural gas import/export facility.

Mr. PFLUGER. So my district, the Permian Basin, 6 million barrels a day, needs to be protected. The authorities in some cases, as you recommended in your testimony, should be delegated to private companies, in some cases, to both identify and also mitigate, if needed.

Mr. BAUMGARTNER. I think that energy infrastructure in your district should be considered to be protected. Now, how that—how that gets to a place where we can do that as the private sector, there are probably steps to get there. You know, we have great relationships with local, State, Federal law enforcement and are happy to take an intermediary step to work with them to ensure that we understand the technology, the appropriate technology is in place, and we can implement that technology in a future state.

Mr. PFLUGER. Thank you.

Dr. Schwennesen, we'll go back to the services for a second and the race for technology. Let's focus on the Air Force, our alma mater, the Air Force Academy.

How would you characterize the responses that we're seeing out of DOD, specifically the Air Force? Are they doing it fast, is it neat in its approach, or is it just average?

Mr. SCHWENNESEN. Right. I think it is below average. It gives me no pleasure to say that, but I think we are not taking it seriously enough.

Again, it is as if everyone sees the train coming, everyone agrees the train is coming, and yet, no one is taking any steps to get out of its way. Everyone is assuming that somebody else is doing it and

there is just no sense of urgency or coherent activity to address this, address this issue. Again, that's easy for me to say. It's easy for me to throw spears from the sidelines.

But I do think that one of the things we can do is leverage our very good relationships we have with Ukraine. We've given them a lot of resources, and they are quite willing and eager to give us something back in return for it. We should be mopping that information up right now. We should be sending people there right now.

Mr. PFLUGER. Thank you very much. My time is expired.

I recognize the Ranking Member for his questions.

Mr. MAGAZINER. Thank you, Chairman, and thank you both.

Dr. Schwennesen, I want to begin by commending you and thanking you for your assistance to the Ukrainians. You know, I have to remind, unfortunately, some of my colleagues from time to time that Vladimir Putin is not our friend, that the cause of the Ukrainians is the cause of freedom and democracy, and that Russia continues to pose a threat not just to Ukraine, but to American interests all over the world.

So I just want to thank you for the work that you're doing over there, because that is the front line of freedom today.

Mr. SCHWENNESEN. Thank you.

Mr. MAGAZINER. I was interested in your written testimony when you expressed some skepticism in the effectiveness of signal-jamming technology to mitigate risks from UAS on the battlefield. I was wondering if you could expand on that.

Why are you sort-of skeptical about the effectiveness or the promise of signal-jamming and other counter-UAS technology on the battlefield, and also writ large?

Mr. SCHWENNESEN. Sure. I claim no engineering expertise in drone warfare, but all I can do is say what I've seen, which is that in the world's most intense EW battle space, which is the Ukrainian Russian front at the moment, it is an electronic warfare chaos, right?

So, what people used to think about the ability to jam drones, which is what some of the speakers we had here are talking about, which is, you know, 2 years old, which at this point is effectively a century-old obsolete information, jamming doesn't work the way we think it does.

There are so many new developing technologies on countering the counters, right? They've already gone multiple layers ahead of us. At this point, they're doing AI pixel-lock technology that doesn't have any RF frequency whatsoever. They're doing ambush technology where they're not needing to have any kind of communication between operator and drone.

So, you know, again, I don't know the specifics beyond what I've just seen the tip of the iceberg, which is that, you know, the jamming solution is not a one-size-fits-all. That's the silver bullet. It might be a piece of a suite, but that's only a piece.

Mr. MAGAZINER. I recognize that you've thought about this in sort of the DOD space more, perhaps, than homeland, you know, domestic law enforcement, et cetera, but I imagine the lessons are transferrable.

What do we need to do specifically in order to go from being laggards to leaders on this? You referenced procurement issues and

kind-of speeding that up. You referenced, you know, bringing a spirit of, I guess, inventiveness and innovation.

But are there other specific things? I mean, is there training that we should be looking at deploying across the Federal Government? Is there some kind of specific workaround to procurement rules that you would recommend? Like, what are the nuts and bolts of what we should be doing in order to take back the advantage?

Mr. SCHWENNESEN. Yes. I do think Yankee ingenuity is one of our comparative strengths, and we need to take advantage of it. One of the ways to do that—this is not an especially sexy solution and, you know, so I say that with apologies in advance, but I think one example of an idea is to, at the DOD level, get drones down to the absolute operational level of unit, so they can begin to tinker.

There is—you know, as Elon Musk says, Move fast and break things. You need to learn on the fly. You need to learn in the trenches how these things are operated. It isn't enough to do this from a centrally-managed top-down approach in which we're going to go through this entire, you know, typical cycle and then deliver the tool to the warfighter, you know, wrapped with a ribbon. It doesn't work that way anymore. We have to give it to them and let them develop it on the fly.

Mr. MAGAZINER. Empower the people on the front lines to innovate. That makes sense.

Mr. Baumgartner, I apologize, I only have a minute left, but I wanted to explore this importance of cooperation between private industry and particularly State and local law enforcement.

What are the best practices there that you've noticed, and are there things that we can do to support those kinds of collaborations?

Mr. BAUMGARTNER. Well, we work very hard to establish and maintain those relationships in all the States and localities that we serve. I think it is—it does become about manpower and hours spent in doing that collaboration.

So, there are certainly challenges to maintaining that, but I think fusion centers are a great opportunity to engage in a wide variety of State and local efforts at one location. I think there are other similar opportunities.

Like, in our sector we have the Electricity Information Sharing and Analysis Center, that also convenes those State and local partners in a regional fashion, and we're able to effectively have those conversations and maintain those relationships in that forum as well.

Mr. MAGAZINER. Thank you both.

Mr. PFLUGER. Thank you, Ranking Member.

I now recognize myself for 5 minutes, and I'm not going to take 5 minutes.

But, Mr. Schwennesen, I totally agree with you that we have a problem here in the United States in dealing with these systems, not only for warfare, but also for protecting the homeland.

I would think that what—part of the problem is that you got $500,000 in the FBI, I'm sure you have $500,000 in some other agency, and you got all these agencies working on the same issue and it's not really centralized.

There's no planning, et cetera. Maybe airports are trying to do their thing, and the FBI is trying to do their thing, and Customs and Border Protection is trying to do their thing.

Would it be beneficial to try to put this all together and just focus on the unmanned aerial system threat in the homeland?

Mr. SCHWENNESEN. I have to say I lean that way. I hate to beat a dead horse here, but the Ukrainians have, once again, shown some ways to deal with this. They have stood up their entire separate new force, very much like the Marine Corps or the Air Force. They've set up the Unmanned Aerial Systems Service in the Ukrainian Department of Defense in order to do precisely that, in order to address this entire new sector of technology and how it's to be developed and applied.

Mr. PFLUGER. Probably one of the advantages that the Ukrainians had is that they had no Air Force, basically, right? So, by necessity, they needed to come up with something different that actually combated the threat.

We have an Air Force. Unfortunately, what happens is that you have the resistance to change. UAS, unmanned systems, et cetera, are a threat to the people that fly the planes, OK?

So we do need to look at this in an entirely—an entirely different way, and so not only on the DOD side, where we do need to have the private-sector innovate. The RFP should be, Hey, I want to knock out—I want to sink Chinese ships, all right, and just as simple as that.

If you ask DOD to do that, they'll come up with an aircraft carrier that costs $10 billion and all these, you know, systems. The Ukrainians are sinking Russian ships in the Black Sea with the little boats with, you know, maybe 5- or 600 pounds of TNT on them, a whole bunch of them. You can't possibly take them all out, and basically boom.

No submarine, because that's the other thing we need to look at. Well, maybe we need to, you know, have these really expensive submarines with torpedoes and stuff, the old way of fighting war. We need to look at the new way of fighting war. But here, it's Homeland Security.

Look, I'm convinced that we're going to have a problem. We'll wake up when something happens, because that's always what we do. We should be waking up right now.

So one of the things maybe that we should be looking at is how do we centralize a Homeland Security kind of focus on unmanned systems and how we protect all our infrastructure, airports, you know, the energy system, our electricity, our grid, all that. All that is vulnerable. So, you know, that's all I have to say.

I'll yield my time back. I recognize the gentleman from New York, Mr. D'Esposito.

Mr. D'ESPOSITO. Thank you, Mr. Chairman.

Mr. Schwennesen, I know it was discussed earlier, and I wish some of those on the other side were here to listen, because sometimes when we talk about Russia, China, and Iran, we're, you know, referred to as fear mongers. But the proliferation of drone technologies from foreign adversaries like Russia, like China, like Iran has impacted conflicts across the globe.

What is the risk of such technology being transferred or replicated by domestic actors in the United States, or by transnational criminal organizations across our borders? How can we disrupt the supply chains?

Mr. SCHWENNESEN. Well, the risk is 100 percent. I mean, if it hasn't happened already—I'm sure it has, but if it hasn't, it's about to happen.

Mr. D'ESPOSITO. Definitely has.

Mr. SCHWENNESEN. Right, right. How do we mitigate it is—again, this is the elephant in the room. I think the only way to mitigate these kind of threats is to out-innovate the threat itself. This is something that we've been traditionally good at. It's something that we have the technical know-how and the capacity to do. Right now we just have not opened the gates. We have not gotten our juices flowing, as they say, to address these threats and out innovate the threat.

Mr. D'ESPOSITO. Thank you.

I know we have to go vote, so I'm going to make this quick. But, Mr. Baumgartner, just last month a Tennessee man was arrested for plotting to use a drone carrying an explosive to destroy a national power substation. We know that there have been additional incidents of suspicious drone activity near substations. I think this is critically important, especially in the time we are in where there is this big push for alternate energy sources, whether it's battery storage, whether it's wind storage, without really doing the work to make sure that we can protect these assets.

In addition to cyber concerns, what physical security risks do drones pose to energy sector assets?

Mr. BAUMGARTNER. A great question.

I think payloads are, obviously, as witnessed in the Tennessee case, but you could simply ram a drone into some of our infrastructure. We do take a defense, in-depth approach and try to add shielding and obfuscate certain targets. But on top of that you could also see a situation and we've seen published cases where they've actually used drones to enable a cyber intrusion as well.

Mr. D'ESPOSITO. Thank you.

Mr. Chairman, I yield back.

Mr. GIMENEZ. I thank the gentleman from New York.

I thank all of the witnesses for their valuable testimony and the Members for their questions.

The Members of the subcommittee may have some additional questions for the witnesses, and we would ask the witnesses to respond to these in writing.

Pursuant to committee rule VII(D), the hearing record will be held open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 4:37 p.m., the subcommittee was adjourned.]

APPENDIX

LETTER FROM THE U.S. CHAMBER OF COMMERCE

December 9, 2024.

The Honorable AUGUST PFLUGER,
Chairman, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence, U.S. House of Representatives, Washington, DC 20515.

The Honorable SETH MAGAZINER,
Ranking Member, Subcommittee on Counterterrorism, Law Enforcement, and Intelligence, U.S. House of Representatives, Washington, DC 20515.

The Honorable CARLOS GIMENEZ,
Chairman, Subcommittee on Transportation and Maritime Security, U.S. House of Representatives, Washington, DC 20515.

The Honorable SHRI THANEDAR,
Ranking Member, Subcommittee on Transportation and Maritime Security, U.S. House of Representatives, Washington, DC 20515.

DEAR CHAIRMEN PFLUGER AND GIMENEZ, AND RANKING MEMBERS MAGAZINER AND THANEDAR: The U.S. Chamber of Commerce ("Chamber") respectfully submits the following statement for the record for the House Homeland Security Subcommittee Counterterrorism, Law Enforcement, and Intelligence and Transportation Maritime's joint hearing titled "Safeguarding the Homeland from Unmanned Aerial Systems." We appreciate the committees' on-going efforts to address the public safety threats posed by illicit unmanned aircraft, or drones, to our Nation's critical infrastructure, sporting and entertainment events, and airports.

Drones provide substantial economic, social, and national security benefits to the United States and it is crucial that we take a global lead in this innovative technology. However, the potential misuse and illicit use of drones presents major public safety, national security, and economic concerns. These concerns include endangering the flying public, disrupting major sporting and entertainment events, enabling criminal and terrorism threats to public safety, and espionage of our most advanced critical infrastructure facilities. These risks are not hypothetical, given the number of unauthorized drone intrusions, close calls, and use of drones globally for malicious purposes.[1]

Presently, four Federal agencies have the legal authority to utilize counter-drone detection and mitigation technologies to protect certain sensitive facilities and operations. While we support the missions of those Federal agencies to use counter-drone technologies, those Federal agencies do not have sufficient resources and adequate legal authorities to fully protect the full scope of sensitive facilities and operations. Congress can remedy this issue by responsibly expanding detection and mitigation authorities to other key Federal Government agencies and functions that currently do not possess these authorities, detection authorities for private-sector enti-

[1] Sara Ruberg, *Man Planned to Use Drone With Explosive to Attack Substation, U.S. Says,* THE NEW YORK TIMES (Nov. 4, 2024), *https://www.nytimes.com/2024/11/04/us/columbia-energy-facility-weapon-mass-destruction.html;* James Tutten, *FBI Investigates After Large Drones Seen Flying Near Military Base and Trump's Bedminster Golf Club,* WFTV9 (Dec. 4, 2024), *https://www.wftv.com/news/local/fbi-investigates-after-large-drones-seen-flying-near-military-base-trumps-bedminster-golf-club/UU7N062Y6VAZNCM18N3G07XYT4/*; Gordon Lubold, Lara Seligman, and Aruna Viswanatha, *Mystery Drones Swarmed a U.S. Military Base for 17 Days. The Pentagon Is Stumped,* THE WALL STREET JOURNAL (Oct. 12, 2024), *https://www.wsj.com/politics/national-security/drones-military-pentagon-defense-331871f4: Russian Drones Attack Critical Infrastructure in Ukraine's West, Air Force Says,* REUTERS (Dec. 2, 2024), *https://www.reuters.com/world/europe/russian-drone-attack-leaves-parts-ukraines-ternopil-without-power-military-says-2024-12-03*; UAS Sightings Report, Federal Aviation Administration (accessed Dec. 9, 2024), *https://www.faa.gov/uas/resources/public_records/uas_sightings_report.*

ties, and limited mitigation authority for State and local enforcement through a pilot program. Expanding the aperture of entities that possess counter-drone authorities conserves limited Federal resources and empowers Federal agencies to prioritize protecting the most sensitive assets and operations.

We recognize the complexities presented by employing counter-drone technologies, and support placing reasonable and tailored guardrails on expanded counter-drone use to address important policy goals including protecting privacy and civil rights, ensuring aviation safety, addressing spectrum interference, continuing Federal oversight of the national air space, and allowing lawful commercial activity. However, policy makers should ensure that any counter-drone framework minimizes red tape for law enforcement and the private sector while also being practical to implement, otherwise, the benefits of expanded detection and mitigation authorities will not be realized.

Ensuring public safety and the security of the national air space is an important priority for the U.S. Chamber, and a tailored counter-drone framework plays a significant role in achieving that objective. We urge you to act on this important issue.

Sincerely,

TOM QUAADMAN,
Senior Vice President Economic Policy, U.S. Chamber of Commerce.

STATEMENT OF GB JONES, CHIEF SAFETY AND SECURITY OFFICER FOR FIFA WORLD CUP 2026

TUESDAY, DECEMBER 10, 2024

Good afternoon, Chairman Pfluger, Chairman Gimenez, Ranking Member Magaziner, Ranking Member Thanedar, and Members of the subcommittee. I am G.B. Jones, chief safety and security officer for FIFA World Cup 2026 US, Inc. (FWC26). Thank you for the opportunity to provide written testimony on today's hearing about countering unmanned aerial systems (C–UAS).

For over 31 years, I spent my career in Federal, State, and local law enforcement, including as a municipal police officer, deputy sheriff, Minnesota State trooper, and FBI agent. At the FBI, I served in various roles including an assistant special agent in charge, the FBI's on-scene commander during the interagency response to 3 separate mass shooting events, and as the FBI's deputy on-scene commander for counterterrorism operations in Baghdad, Iraq. I also served as the unit chief of the special events management unit at FBI headquarters, where I directed counterterrorism preparedness programs, including those related to special event and aviation security. I was as an FBI pilot and am currently rated as an FAA Part 107 commercial remote pilot.

Before joining FWC26, I worked at the National Football League (NFL) as the director of investigation and security services for international and special events, helping to lead the safety and security efforts around Super Bowls and international NFL games across the globe, including C–UAS efforts. While air space security and safety were the primary concerns, I also developed an appreciation for the many positive uses of commercial drones and pioneered the effort to integrate commercial drones safely and thoughtfully into the secure air space around NFL games and events. This required careful coordination with numerous stakeholders, including Federal, State, and local law enforcement and private security officials, and fundamental air space domain awareness. With respect to drones and other aircraft over our critical infrastructure, it is essential to understand who are the good guys, who are the bad guys, and how to differentiate them. That is the perspective I offer in my testimony to you today.

Over the next 2 years, the United States will be at the center of the world's largest sport—soccer. In the summer of 2025, the United States will host the FIFA Club World Cup, a first-of-its-kind tournament bringing the world's best club teams to the United States to compete in the most inclusive and merit-based global club competition in history. Sixty-three matches will be played in 12 stadiums in 11 cities in the United States. The following summer in 2026, Canada, Mexico, and the United States will host the FIFA Men's World Cup, which will be the largest, most-watched sporting event in history, with 104 matches taking place throughout North America. The United States will hold 78 of these matches across 11 U.S. host cities and will host almost all 48 eligible teams at base camps across the Nation, delivering an enormous economic opportunity for communities and businesses across all industries.

In addition, the FIFA Club World Cup 2025 and the FIFA World Cup 2026 will kick off a mega decade of global sports in the United States—bringing large-scale

soccer tournaments, the LA 2028 Summer and the Salt Lake City 2034 Winter Olympic Games, Rugby World Cups, and other events to our country.

In preparation for the 2 tournaments, FWC26 is responsible for organizing the FIFA Club World Cup 2025 and the FIFA World Cup 2026, and safety and security remain top priorities. Drones are one of the major security challenges. We are concerned about nefarious payloads, WMD and HazMat threats, intellectual property rights theft, and other security threats. But we are also keenly focused on safety threats associated with illegal drone activity. In 2016, a EURO 2016 match between Albania and Serbia was abandoned after a drone carrying a political banner caused a mass brawl on the pitch. In 2019, a La Liga Match between Athletic Bilbao and Real Madrid was suspended after a drone carrying a political banner ignited passions and interrupted the game. Safety and security threats to the FIFA Club World Cup 2025 and FIFA World Cup 2026, and the use of UAS as a threat vector, remain significant concerns.

The threat posed by drones has been well-documented, and for at least the last 4 years, potential solutions have been articulated to Congress through studies, hearings, and other efforts. To date, no action has been taken on one of the most important recommendations—expansion of response and mitigation authorities beyond Federal authorities to State, local, Tribal, and territorial partners.

I am concerned about the capacity of U.S. Federal law enforcement to protect the upcoming sporting events with enough cUAS equipment and trained personnel. Unlike multi-jurisdictional resource-sharing agreements, Emergency Management Assistance Compacts, and other mutual aid agreements which can be leveraged to mitigate other threats, there is no mechanism for the Federal Government to seek and receive support to manage the UAS threat from any other partners. There is a clear solution. Skilled State, local, Tribal, and territorial officers see threats beyond their communities. They are better trained and better informed than ever before. They think globally, and act locally. Yet they are powerless to respond to UAS threats because Congress has not acted to empower law enforcement authorities outside the Federal Government to address UAS threats in their local communities.

Successful UAS threat mitigation for the Club World Cup and World Cup will require collaboration between private-sector vendors, security teams, and all law enforcement jurisdictional levels. There are models for this kind of collaboration in the FBI's Joint Terrorism Task Forces, in the public safety bomb technician program, and in other multi-jurisdictional, inter-disciplinary task forces where Federal, State, and local law enforcement and homeland security partners train to the same standard, are equipped with compatible and interoperable equipment, and deploy with the requisite authorities to mitigate the threats. We must look at these models for guidance in addressing the UAS threat.

Over the next 2 years, the FIFA Safety and Security Department will focus on strategies and innovative approaches to bolster UAS threat detection and response capabilities. We will work with Federal partners to request Temporary Flight Restrictions (TFRs) that will create the "authority to act" against criminal drone intrusions. We will work with law enforcement partners to conduct comprehensive assessments of the stadiums to identify and patrol logical launch and land locations, we will placard "no drone zones," we will embark on education campaigns and public service announcements, and we will work with stadiums to enhance technical capabilities to detect drones. We will create UAS response strategies which integrate technology and human factors, we will train security and local law enforcement, and we will exercise our protocols to minimize the time from identification to response. But none of these things permit the local law enforcement partners who are embedded in stadium command posts with us to take definitive action against rogue drones which may be bearing down on our matches in defiance of the law, the placards, and the education campaigns. We need Congress's help.

As a first step, Congress should reauthorize the Preventing Emerging Threats Act to renew the authorities granted to Federal partners to mitigate drone threats. This is necessary to preserve the ability of Federal law enforcement to respond to current threats. As a complement to this, we support pending requests from the Department of Homeland Security (DHS) for additional resources for training, equipment, and personnel for counter-UAS (cUAS) operations which will benefit protection of the FIFA Club World Cup, World Cup, and other major events. Thoughtfully, the DHS cUAS Program Office has articulated a plan to build the cUAS capacity of several key DHS component agencies to address drone threats more effectively within their areas of jurisdiction. These same resources could then be activated in tandem to deploy to protect major special events or critical infrastructure as a single, unified, and interoperable cUAS task force. At the conclusion of the incident or event, cUAS personnel would return to their component agencies to resume their normal duties.

This plan builds capacity and resilience in the components, and across DHS, beyond anything that exists in U.S. Government cUAS operations today.

Following reauthorization of current authorities, we urge Congress to consider future reauthorizations with a longer term of effectiveness. This would send a strategic signal to Federal agencies that the UAS threat merits an investment in time, training, resources, and capital improvements. With a long-term strategy, Federal agencies would be encouraged to plan beyond the 1-year cycle to focus on development of training, technology, and mitigation tools and strategies that would lead to more robust defenses against UAS threats. The United States is playing host to large-scale, international sporting events nearly every year for the next 10 years. Strategic leadership and thoughtful investment in cUAS efforts will pay protective dividends for at least the next decade.

Finally, we ask Congress to consider expanding mitigation authority to appropriately-trained and equipped State, local, Tribal, and territorial law enforcement partners. Informed by Federal guidance and leadership, the development of consistent training, selection of interoperable tools, and creation of compatible response policies across multiple State, local, Tribal, and territorial agencies will create a fabric of cUAS responders with the expertise to respond to drone threats across the country. This will not only build capacity in individual communities, but through interoperable processes and procedures, Federal, State, local, Tribal, and territorial officers will have the ability to couple their efforts to protect against threats to international special events and respond to incidents of national significance such as natural disasters or criminal or terrorist attacks.

In closing, the United States has an incredible opportunity in the next decade to leverage large-scale sporting events like the FIFA Club World Cup 2025 and the FIFA World Cup 2026 for generational, positive economic impacts. To ensure communities across our country realize those impacts, delivering safe and secure sporting events is paramount. We look forward to working with the committee, Congress, and the Federal Government to deliver the safe and exciting tournaments in 2025 and 2026.

Thank you to the Chairmen for the invitation and thank you to the Members for your time.