SURVEILLANCE, SABOTAGE, AND STRIKES: INDUSTRY PERSPECTIVES ON HOW DRONE WARFARE ABROAD IS TRANSFORMING THREATS AT HOME

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JULY 15, 2025

Serial No. 119–21

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

61–404 PDF WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

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

MICHAEL T. MCCAUL, Texas, *Vice Chair*
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona
ANDREW OGLES, Tennessee
SHERI BIGGS, South Carolina
GABE EVANS, Colorado
RYAN MACKENZIE, Pennsylvania
BRAD KNOTT, North Carolina

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
ERIC SWALWELL, California
J. LUIS CORREA, California
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
DANIEL S. GOLDMAN, New York
DELIA C. RAMIREZ, Illinois
TIMOTHY M. KENNEDY, New York
LAMONICA MCIVER, New Jersey
JULIE JOHNSON, Texas, *Vice Ranking Member*
PABLO JOSÉ HERNÁNDEZ, Puerto Rico
NELLIE POU, New Jersey
TROY A. CARTER, Louisiana
AL GREEN, Texas
VACANCY

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

CARLOS A. GIMENEZ, Florida, *Chairman*

ANDREW R. GARBARINO, New York
ELIJAH CRANE, Arizona
SHERI BIGGS, South Carolina
MARK E. GREEN, MD, Tennessee *(ex officio)*

LAMONICA MCIVER, New Jersey, *Ranking Member*
TIMOTHY M. KENNEDY, New York
TROY A. CARTER, Louisiana
BENNIE G. THOMPSON, Mississippi *(ex officio)*

ROLAND HERNANDEZ, *Subcommittee Staff Director*
ALEX MARSTON, *Minority Subcommittee Staff Director*

CONTENTS

SURVEILLANCE, SABOTAGE, AND STRIKES: INDUSTRY PERSPECTIVES ON HOW DRONE WARFARE ABROAD IS TRANSFORMING THREATS AT HOME

Tuesday, July 15, 2025

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

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 310, Cannon House Office Building, Hon. Carlos A. Gimenez (Chairman of the subcommittee) presiding.

Present: Representatives Gimenez, Garbarino, Crane, Biggs of South Carolina, McIver, Kennedy of New York, and Carter of Louisiana.

Also present: Representative Pfluger.

Mr. GIMENEZ. The Committee on Homeland Security Subcommittee on Transportation and Maritime Security will come to order.

Without objection, the Chair may declare the subcommittee in recess at any point.

Today's hearing is examining how drone warfare tactics used abroad are transforming threats to our homeland.

From Ukraine to the Middle East, our adversaries are deploying increasingly sophisticated drone capabilities that can be adapted by terrorists, lone actors, or State proxies within the United States.

This hearing will explore how industry leaders are innovating to help close critical security gaps and better protect our transportation systems and infrastructure.

Without objection, the gentleman from Texas, Mr. Pfluger, is permitted to sit with the subcommittee and ask questions of the witnesses.

I now recognize myself for an opening statement.

Good morning. I want to thank everyone for joining us for today's hearing, which will examine how drone warfare overseas is reshaping the threat environment here at home.

In recent years, the use of unmanned aircraft systems—or drones—by foreign adversaries, terrorist groups, and proxy forces has grown significantly.

Once confined to distant battlefields, these platforms are now being deployed in ways that challenge traditional security assumptions and expose critical vulnerabilities across our homeland.

Drones have become essential tools of modern warfare. On the battlefields of Ukraine, both Russian and Ukrainian forces are deploying thousands of drones not only for surveillance and artillery targeting, but for direct offensive operations.

These include quadcopters assembled from commercial parts, long-range loitering munitions, and first-person-view kamikaze drones enhanced by open-source software. They are low-cost, adaptable, and increasingly precise.

Just weeks ago, Ukraine launched a deep strike inside Russian territory using a coordinated wave of drones, damaging strategic bombers thousands of miles from the front lines.

Russia continues to rely on Iranian-made Shahed drones to bombard Ukrainian energy infrastructure, saturate air defenses, and inflict lasting psychological and economic harm.

In the Middle East, Iranian-backed groups such as Hezbollah and the Houthis have demonstrated the operational reach and lethality of these systems. They have targeted U.S. service members, international shipping, and critical infrastructure.

The drone strike that killed 3 American service members in Jordan in early 2024 underscored just how dangerous and asymmetric this threat has become.

More recently, during a 12-day conflict last month, Israel launched a series of drone and missile strikes against Iranian military sites, some originating from launch points within Iran itself, illustrating how even layered air defense systems can be bypassed using prepositioned commercial technologies.

What makes these developments more alarming is the accessibility of the technology. Many of the systems deployed abroad are constructed using commercially-available components and open-source software.

These tools are not limited to nation-states. Lone actors, extremists, networks, and transnational criminal organizations can easily acquire and weaponize drones with minimal cost and training.

Here in the United States the warning signs are emerging. Reports of unauthorized drone activity near airports and other critical infrastructure are becoming more frequent. Hundreds of sightings have been documented near military installations and sensitive energy facilities in the past year alone.

The potential for a coordinated drone attack on an airport, seaport, or mass gathering is a credible and growing threat.

My home district in South Florida is particularly exposed. With major transportation hubs like Miami International Airport, the Port of Miami, and a dense network of energy and telecommunications infrastructure, we are a high-profile target.

A single drone equipped with an explosive device or electronic warfare payload could cause significant disruption, physical damage, and wide-spread panic.

We cannot afford to be reactive. The time to act is now.

Another concern is the wide-spread presence of Chinese-manufactured drones operating within the United States.

DJI, a company based in Communist China, commands a significant share of both the global and U.S. commercial drone market. Its platforms are used by private industry, lobbyists, and even some public safety agencies.

In fact, even several DHS components have—inexplicably—used DJI's AeroScope system to monitor drone activity near sensitive locations.

While AeroScope may offer affordable situational awareness, it also raises serious concerns about the national security risks posed by Chinese-linked technology, especially regarding data access, remote control capabilities, and potential sabotage during a future crisis or conflict with China.

Today's hearing will explore what the private sector is experiencing on the front lines of drone security, the counter-UAS tools that are currently available, and the extent to which Federal, State, and local authorities are equipped with the legal and operational capabilities to address these threats.

At present, the Department of Homeland Security has limited authorities to disrupt or disable malicious drone activity. Most State and local law enforcement agencies have no authority whatsoever.

This is a glaring gap in our national preparedness, one that we must urgently address as we prepare to host globally significant events like the 2026 FIFA World Cup and the 2028 Summer Olympics.

We'll also hear testimony on the broader risks posed by Chinese-made drones collecting sensitive location data across the United States. These systems could be used for surveillance or even to carry out attacks.

This is not simply a question of data privacy. It's a matter of homeland security.

Our adversaries are adapting rapidly. Our defenses must keep pace. That means updating our legal authorities, investing in next-generation detection and mitigation tools, and partnering closely with industry and State and local stakeholders.

I want to thank our witnesses for appearing before the subcommittee today and for their continued efforts to keep our Nation secure. Your perspectives will help inform the committee's work as we seek to close dangerous gaps before they are exploited.

I look forward to your testimony and to a productive discussion. Thank you.

[The statement of Chairman Gimenez follows:]

STATEMENT OF CHAIRMAN CARLOS GIMENEZ

JULY 15, 2025

Good afternoon. I want to thank everyone for joining us for today's hearing, which will examine how drone warfare overseas is reshaping the threat environment here at home.

In recent years, the use of unmanned aircraft systems, or "drones", by foreign adversaries, terrorist groups, and proxy forces has grown significantly. Once confined to distant battlefields, these platforms are now being deployed in ways that challenge traditional security assumptions and expose critical vulnerabilities across our homeland.

Drones have become essential tools of modern warfare. On the battlefields of Ukraine, both Russian and Ukrainian forces are deploying thousands of drones not only for surveillance and artillery targeting, but for direct offensive operations. These include quadcopters assembled from commercial parts, long-range loitering munitions, and first-person-view kamikaze drones enhanced by open-source software. They are low-cost, adaptable, and increasingly precise.

Just weeks ago, Ukraine launched a deep strike inside Russian territory using a coordinated wave of drones, damaging strategic bombers thousands of miles from

the front lines. Russia continues to rely on Iranian-made Shahed drones to bombard Ukrainian energy infrastructure, saturate air defenses, and inflict lasting psychological and economic harm.

In the Middle East, Iranian-backed groups such as Hezbollah and the Houthis have demonstrated the operational reach and lethality of these systems. They have targeted U.S. service members, international shipping, and critical infrastructure. The drone strike that killed 3 American service members in Jordan in early 2024 underscored just how dangerous and asymmetric this threat has become.

More recently, during a 12-day conflict last month, Israel launched a series of drone and missile strikes against Iranian military sites, some originating from launch points within Iran itself, illustrating how even layered air defense systems can be bypassed using prepositioned commercial technologies.

What makes these developments more alarming is the accessibility of the technology. Many of the systems deployed abroad are constructed using commercially-available components and open-source software. These tools are not limited to nation-states. Lone actors, extremist networks, and transnational criminal organizations can easily acquire and weaponize drones with minimal cost and training.

Here in the United States, the warning signs are emerging. Reports of unauthorized drone activity near airports and other critical infrastructure are becoming more frequent. Hundreds of sightings have been documented near military installations and sensitive energy facilities over the past year alone. The potential for a coordinated drone attack on an airport, seaport, or mass gathering is a credible and growing threat.

My home district in South Florida is particularly exposed. With major transportation hubs like Miami International Airport, the Port of Miami, and a dense network of energy and telecommunications infrastructure, we are a high-profile target. A single drone equipped with an explosive device or an electronic warfare payload could cause significant disruption, physical damage, and wide-spread panic. We cannot afford to be reactive. The time to act is now.

Another concern is the wide-spread presence of Chinese-manufactured drones operating within the United States. DJI, a company based in Communist China, commands a significant share of both the global and U.S. commercial drone market. Its platforms are used by private industry, hobbyists, and even some public safety agencies. In fact, even several DHS components have, inexplicably, used DJI's AeroScope system to monitor drone activity near sensitive locations.

While AeroScope may offer affordable situational awareness, it also raises serious concerns about the national security risks posed by Chinese-linked technology, especially regarding data access, remote control capabilities, and potential sabotage during a future crisis or conflict with China.

Today's hearing will explore what the private sector is experiencing on the front lines of drone security, the counter-UAS tools that are currently available, and the extent to which Federal, State, and local authorities are equipped with the legal and operational capabilities to address these threats.

At present, the Department of Homeland Security has limited authorities to disrupt or disable malicious drone activity. Most State and local law enforcement agencies have no authority at all. This is a glaring gap in our national preparedness, one that we must urgently address as we prepare to host globally significant events like the 2026 FIFA World Cup and the 2028 Summer Olympics.

We will also hear testimony on the broader risk posed by Chinese-made drones collecting sensitive location data across the United States. These systems could be used for surveillance or even to carry out attacks. This is not simply a question of data privacy. It is a matter of homeland security.

Our adversaries are adapting rapidly. Our defenses must keep pace. That means updating our legal authorities, investing in next-generation detection and mitigation tools, and partnering closely with industry and State and local stakeholders.

I want to thank our witnesses for appearing before the subcommittee today and for their continued efforts to keep our Nation secure. Your perspectives will help inform the committee's work as we seek to close dangerous gaps before they are exploited.

I look forward to your testimony and to a productive discussion.

Mr. GIMENEZ. I now recognize the Ranking Member, the gentlewoman from New Jersey, Mrs. McIver, for her opening statement.

Mrs. MCIVER. Good morning. Thank you so much, Chairman.

Thank you to our witnesses for joining us today.

Before turning to the topic of today's hearing, I want to offer my condolences to the families, friends, and loved ones of the children

and other victims lost in the devastating floods in Texas last week. My thoughts and prayers are with all those impacted.

As the affected communities begin to recover from this tragedy, I hope our committee will soon have the opportunity to examine what went wrong and ensure our Government can better respond to future disasters.

I also want to thank the brave first responders who helped prevent further loss of life, including Coast Guard Petty Officer Third Class Scott Ruskan of New Jersey and the other Coast Guard members on board helicopter 6553 who helped save many lives from the floodwaters.

The emergency response in Texas is actually relevant to today's hearing as one helicopter involved in the rescue and recovery operations had to be grounded after a collision with a private drone flying in restricted air space.

The incident goes to show the threats drones can pose even when operators have no ill intent and the need for more robust Government capabilities to address such threats.

In recent years, drone usage has become commonplace across a wide range of applications, from emergency response to photography and news coverage. Drone operations provide benefits to businesses and hobbyists alike.

As drone activity increases, we must ensure the Government has the authorities and resources necessary to take action against drone operators who do not follow the rules, including both careless and clueless operators, as well as those who may seek to use drones to carry out attacks.

Though such large-scale attacks have yet to occur within the United States, our critical infrastructure, mass gatherings, and Government facilities are vulnerable to being targeted, especially by lone-wolf actors.

With the World Cup coming to the United States next year, including to MetLife Stadium in my home State of New Jersey, as well as the Olympics coming in 2028, the need for Congress to extend and expand the Government's counter-drone authorities have never been more pressing.

In October 2018, Congress passed legislation providing the Departments of Homeland Security and Justice with limited authorities to detect, track, intercept, and seize drones.

However, just a few months later, incidents at Gatwick Airport in England and my home airport, Newark Liberty International Airport, displayed the inaccuracy of CUAS capabilities as drones shut down airport operations, disrupting travel for thousands of passengers.

Given this subcommittee's jurisdiction over transportation security, I am hopeful that any expansion of authorities provides a path forward for protecting airports from drones.

Last year, New Jersey was again the focus of media attention as the public reported spotting large numbers of drones and unknown aircraft flying over our State.

Further investigation revealed that the aircraft were most likely authorized flights. But, nevertheless, the incident revealed the Government's lack of domain awareness and capabilities for protecting the national air space.

Moving forward, Congress must act to extend and expand authorities in a matter that provides the capabilities needed to counter the threats we face.

At the same time, we must ensure counter-drone systems are operated in a safe and responsible manner that does not impact the safety of commercial flights or violate individual privacy rights and civil liberties.

I hope the Republican majority will prioritize moving legislation to address counter-drone authority soon.

Thank you again for our witnesses for joining us today.

With that, I yield back.

[The statement of Ranking Member McIver follows:]

STATEMENT OF RANKING MEMBER LAMONICA MCIVER

JULY 15, 2025

Before turning to the topic of today's hearing, I want to offer my condolences to the families, friends, and loved ones of the children and other victims lost in the devastating floods in Texas last week. My thoughts and prayers are with all those impacted.

As the affected communities begin to recover from this tragedy, I hope our committee will soon have the opportunity to examine what went wrong and ensure our Government can better respond to future disasters.

I also want to thank the brave first responders who helped prevent further loss of life, including Coast Guard Petty Officer 3d Class Scott Ruskan and the other Coast Guard members onboard helicopter 6553, who helped save many lives from the flood waters.

The emergency response in Texas is actually relevant to today's hearing, as one helicopter involved in rescue and recovery operations had to be grounded after a collision with a private drone flying in restricted air space. The incident goes to show the threats drones can pose even when operators have no ill intent—and the need for more robust Government capabilities to address such threats.

In recent years, drone usage has become commonplace across a wide range of applications, from emergency response to farming to photography and news coverage. Drone operations provide benefits to businesses and hobbyists alike. As drone activity increases, we must ensure the Government has the authorities and resources necessary to take action against drone operators who do not follow the rules—including both "careless and clueless" operators, as well as those who may seek to use drones to carry out attacks.

Recent drone attacks by Russia, Ukraine, and Israel have displayed how drones can be used in warfare to deadly effect. Though such large-scale attacks have yet to occur within the United States, our critical infrastructure, mass gatherings, and Government facilities are vulnerable to being targeted, especially by lone-wolf actors.

With the World Cup coming to the United States next year—including to MetLife Stadium in my home State of New Jersey—as well as the Olympics coming in 2028, the need for Congress to extend and expand the Government's counterdrone authorities has never been more pressing. In October 2018, Congress passed legislation providing the Departments of Homeland Security and Justice with limited authorities to detect, track, intercept, and seize drones.

However, just a few months later, incidents at Gatwick Airport in England and my home airport of Newark Liberty International Airport displayed the inadequacy of C–UAS capabilities, as errant drones shut down airport operations, disrupting travel for thousands of passengers.

Given this subcommittee's jurisdiction over transportation security, I am hopeful that any expansion of authorities provides a path forward for protecting airports from drones. Last year, New Jersey was again the focus of media attention as the public reported spotting large numbers of drones and unknown aircraft flying over our State. Further investigation revealed that the aircraft were mostly authorized flights, but nevertheless, the incident revealed the Government's lack of domain awareness and capabilities for protecting the national air space.

Moving forward, Congress must act to extend and expand authorities in a manner that provides the capabilities needed to counter the threats we face. At the same time, we must ensure counterdrone systems are operated in a safe and responsible

manner that does not impact the safety of commercial flights or violate individual privacy rights and civil liberties. I hope the Republican Majority will prioritize moving legislation to address counterdrone authorities soon.

Mr. GIMENEZ. I want to thank the Ranking Member.

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

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JULY 15, 2025

I want to begin by offering my condolences to those impacted by the tragic floods in Texas. The loss of life is devastating, and my thoughts are with the victims, survivors, and their families and loved ones. Sadly, the damage wrought by the floods was exacerbated by the Trump administration's mismanaged response. I have called on Chairman Green to immediately convene a hearing to examine the administration's actions to undermine FEMA and our preparedness for the remainder of hurricane season. I hope he will answer that call soon.

In the mean time, today we are here to discuss a different threat to the homeland: the threat posed by unmanned aerial systems or drones. In 2018, Congress enacted the Preventing Emerging Threats Act of 2018, which provided the Departments of Homeland Security and Justice with targeted authorities to detect, track, and mitigate unauthorized drones that pose a threat to certain facilities, assets, and events. These authorities have allowed the Federal Government to begin to develop the testing, policies, and processes to procure and deploy effective counter-UAS systems and technologies.

DHS and DOJ have had some significant successes in protecting high-profile National Special Security Events from unauthorized drone incursions. However, the use of drones has continued to proliferate rapidly, both domestically and abroad. Drones are used for a wide variety of purposes across many sectors, including in emergency response, agriculture, law enforcement, photography, and package delivery. Drones have also been used in warfare by the United States and our allies and adversaries alike, providing militaries and intelligence agencies with a novel tool for intelligence, surveillance, reconnaissance, interference, and kinetic attacks. Though the vast majority of drone use within the United States is harmless and law-abiding, the use of drones in warfare abroad makes clear the potential threats drones may pose to the homeland.

The potential for bad actors to use drones to carry out attacks on mass gatherings, critical infrastructure, and other targets necessitates the extension and expansion of authorities for the Federal Government and law enforcement partners to detect, track, intercept, and seize unauthorized drones flying in restricted air space. The Government must have the ability to respond to developing threats and prevent attacks. At the same time, authorities must be expanded in a manner that protects individuals' privacy and due process rights, as well as the safety of the national air space. Already, we have seen the potentially damaging effects counter-drone technologies can have when operated without appropriate coordination.

Earlier this year, the U.S. Secret Service allegedly operated a C–UAS system without clearance from the Federal Aviation Administration, resulting in inappropriate automated alerts to several pilots flying aircraft near Ronald Reagan Washington National Airport, which could have undermined flight safety. Over the past several years, I have worked in a bipartisan manner with colleagues across the committees with shared jurisdiction to develop legislation to extend and expand counterdrone authorities in a significant yet thoughtful manner. Last Congress, Chairman Green introduced H.R. 8610, the Counter-UAS Authority, Security, Safety, and Reauthorization Act, which I supported as a cosponsor.

The bill would have extended and expanded C–UAS authorities in several key ways, including by establishing a DHS pilot program for State and local law enforcement agencies to receive counterdrone mitigation authorities. The Transportation and Infrastructure Committee reported the bill with bipartisan support last September, but House Republican leadership never called the bill up for floor consideration. I have continued to work with my colleagues to refine the legislation and expect we will reintroduce a version of it soon. I hope the Republican Majority will act swiftly to advance the bill to the floor, through the House, and ultimately into law.

The threats posed by drones are too critical for Congress to wait, especially given the need to protect upcoming events including the World Cup and the Olympics.

Thank you again to our witnesses for joining us today to discuss these critical challenges.

Mr. GIMENEZ. I'm pleased to have a distinguished panel of witnesses before us today on this critical topic.

I ask that our witnesses please rise and raise their right hands.

[Witnesses sworn.]

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

Thank you, and please be seated.

I would now like to formally introduce our witnesses.

Mr. Church Hutton serves as AeroVironment's chief growth officer, a role he assumed in May 2025 to lead the company's strategic expansion and long-term growth initiatives.

Prior to this, he served as senior vice president of government relations, marketing, and communications beginning in 2024 where he played a key role in shaping AeroVironment's public profile and strengthening relationships with government stakeholders.

A retired Army officer and combat veteran, Mr. Hutton spent a decade in senior staff positions on Capitol Hill, including on the professional staff of the Senate Appropriations and Senate Armed Services Committees.

Mr. Tom Walker is the founder and chief executive officer of DroneUp, a leading U.S.-based drone technology company specializing in advanced American-made unmanned aerial systems and integration services.

Under his leadership, DroneUp has become a key industry innovator, supporting a wide range of mission-critical operations, including border security, emergency response, infrastructure monitoring, and last-mile logistics.

Prior to founding DroneUp, Mr. Walker served nearly 17 years as a U.S. Navy officer where he led efforts to modernize digital systems and enhance operational support for the United States and allied special operations forces.

Mr. Brett Feddersen serves as the vice president for strategy and governmental affairs at D-Fend Solutions, where he oversees the company's strategy, public policy, and engagement with U.S. Government agencies, policy makers, and regulators.

Prior to joining the private sector, he held senior executive roles across the Federal Government, including the Federal Aviation Administration, the Department of Defense, and the White House. He is also a retired U.S. Army lieutenant colonel and a former Pennsylvania State trooper.

Mr. Michael Robbins is president and chief executive officer of the Association for Uncrewed Vehicle Systems International, the world's largest trade association for uncrewed systems, robotics, and autonomous technologies, representing companies in both the commercial and defense sectors.

He joined the Association for Uncrewed Vehicle Systems International in 2020 and previously served as chief advocacy officer. Michael is also presently serving as an officer in the United States Navy Reserve.

I thank each of our distinguished guests for being here today.

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

STATEMENT OF PAUL CHURCHILL HUTTON, IV, CHIEF GROWTH OFFICER, AEROVIRONMENT, INC.

Mr. HUTTON. Thank you, Mr. Chairman.

Chairman Gimenez, Ranking Member McIver, and distinguished Members of the subcommittee, thank you for the opportunity to testify on drone warfare abroad and how it's informing domestic investments that will help us prepare for threats here in the United States.

I commend the committee's focus on these challenges and your efforts to enhance the safety of the American people and U.S. transportation systems.

My name is Church Hutton. I serve as the chief growth officer at AV, formerly AeroVironment. It is my pleasure to testify alongside my industry partners in highlighting the challenges and opportunities of providing effective capabilities to our service members and first-line responders in light of the lessons learned from drone warfare abroad.

By way of background, AV is the top producer and supplier by volume of unmanned aerial systems, or UAS, to the Department of Defense, as well as the leading provider of counter-UAS solutions deployed overseas actively protecting Americans, allies, and critical infrastructure abroad. This gives us a holistic view of UAS threats, mitigation tools, and the implications for both to U.S. homeland security.

With major public events on the near horizon, including the World Cup, as you said, Chairman, America's 250th anniversary celebrations, and the 2028 Summer Olympics, we have a collective need to apply these lessons to address threats to U.S. infrastructure and public safety.

Collaboration between Congress and industry is essential to ensure the safety of the American people and critical infrastructure from the evolving threat.

Effective collaboration has a few basic tenets. The first is that we learn the lessons of the foreign drone experience; that authorities are granted to Federal and State agencies to deploy safe and effective UAS solutions in what are clearly complex jurisdictional scenarios; and finally, that Congress provide flexible funding so that Government agencies can validate and adopt technology quickly.

State and non-State actors have increased access to drone capabilities and have demonstrated their ability to achieve lethal effects.

The rapid evolution of small drone systems in conflicts, as demonstrated by Operation Spider's Web in Ukraine and of course Israel's recent campaign against Iran, emphasized the need for agile real-time collaboration to field detection and interdiction tools.

These threats, of course, are not limited to overseas conflicts. UAS increasingly threaten U.S. critical infrastructure with techniques like drone swarming and GPS and radar jamming.

Recent aerial intrusions highlight the need for advanced detection and mitigation technologies to protect our space and maritime domains.

Additionally, acquisition processes must evolve to deliver necessary capabilities. We advocate for agile development and deploy-

ment of affordable open systems, clear operational authorities, and Government-industry partnerships to address these threats effectively.

U.S.-based defense innovators have developed systems to detect, track, and counter these threats that you'll hear about today.

To meet these challenges, the defense industrial base requires strong demand signals, enabling policies, and streamlined authorities. We must act decisively to prevent foreign battlefield lessons from becoming domestic threats.

AV and other innovative companies stand ready to collaborate and provide solutions, but policy inertia and acquisition drag remain significant obstacles.

Collectively, we'll either address these issues now, before we suffer a major drone attack in the homeland, or we'll address them afterward, but certainly we will have to address them.

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

[The prepared statement of Mr. Hutton follows:]

PREPARED STATEMENT OF PAUL CHURCHILL HUTTON, IV

8 JULY 2025

Chairman Gimenez, Ranking Member McIver, and distinguished Members of the subcommittee, thank you for the opportunity today to testify on how drone warfare abroad is transforming and informing domestic investments to prepare for threats here in the United States. I commend this committee's focus on these national security challenges along with your efforts to enhance the safety of U.S. transportation systems. The collaboration between Congress and industry is essential to keeping the American people and critical national infrastructure safe from today's rapidly-evolving drone threats.

AV has a unique vantage point in this space as the top producer and supplier of Unmanned Aerial Systems (UAS) to the Department of Defense (DoD) coupled with our layered counter-UAS solutions deployed to multiple conflict zones abroad. This gives us a holistic view of the UAS threats, mitigation tools, and relevant implications for homeland security. The lessons we have learned from operations abroad underscore the urgent need to address this threat with greater speed and resolve to protect critical U.S. infrastructure and public safety including at high-visibility events like the 2026 FIFA World Cup, America's 250th birthday celebrations, and the 2028 Summer Olympics. In order to accomplish this goal, we believe it is vital that the U.S. Government and Industry have 3 key things in place: (1) a resolve to adopt lessons learned from real operational feedback; (2) flexible sources of funding to modify or scale up the production and delivery of new, software-defined platforms that can be updated in response to evolving threats, and (3) the necessary authorities to allow Federal and State government users to employ technology solutions in what we know are complex jurisdictional scenarios.

THREATS AND EVOLVING ENVIRONMENT

As a former soldier who benefited from DoD's nascent UAS arsenal over 2 decades ago, I commend this panel for bringing awareness to the American people regarding the proliferation of UAS technology—particularly how its capability, lethality, availability, and quantity, when combined, can enable malign actors to threaten unprotected infrastructure and lives.

Looking abroad, Ukraine's recent "Operation Spider's Web" against Russia's strategic bomber infrastructure demonstrated the precision, reach, and destructive ability of small UAS. Spider's Web highlighted the rapid evolution of small drone system capabilities at an affordable cost. The reports of covert Ukrainian launches from inside Russia emphasize the need for agile, real-time Government and industry collaboration to develop detection systems and interdiction tools here at home. Municipal, State, and Federal agencies need to adequately prepare for unmanned and increasingly autonomous systems in their public safety and security strategies.

More recently, in June 2025, during a 12-day conflict with Iran, Israel coordinated a drone and missile campaign targeting Iranian air defenses, ballistic missile plat-

forms, and command infrastructure. While Israeli fighter jets visibly degraded Iran's missile sites and attacked military personnel, Israeli drones, pre-positioned quadcopters, and internet-connected launch platforms operated from within Iran, showcasing this new frontier of drone warfare.

The implications for the defense of our homeland is significant. The use of drones built from commercial parts and operated with minimal infrastructure is increasingly plausible by proxy networks or lone actors on domestic soil. Techniques like drone swarming, GPS jamming, and antiradar flights, perfected abroad, could be adapted to threaten critical U.S. infrastructure.

In the maritime environment, UAS pose a significant threat to shipping in vital trade chokepoints. From 2023 to 2024, there were over 50 UAS incidents in the Red Sea, many involving direct attacks or surveillance of commercial vessels. The increasing frequency and sophistication of these drone operations, by state and non-state actors alike, highlight the urgent need for improved countermeasures to protect critical maritime infrastructure.

Closer to home, unidentified aerial objects have reportedly entered U.S. air space off the East Coast and have raised national security concerns. From 2021 to 2024, over 30 incidents were reported, with objects demonstrating advanced maneuverability and speed. These incursions underscore the critical need for advanced detection and mitigation technologies to protect key maritime regions and ensure U.S. air space security.

Activities at the Southern Border continue to pose a direct threat to our homeland, as transnational criminal organizations, gangs, and extremist organizations adopt UAS to aid in their transport of illicit material into the United States. The defense industrial base is poised to work with Congress and our Executive branch counterparts to ensure we are prepared for UAS incursions and possible attacks through our own borders.

Many of your industry partners recognize these threats and are developing robust countermeasures today. Although these investments are taking place, many challenges remain—requiring Congressional, Federal Executive, plus State, local, and municipal action.

CHALLENGES

Traditional defense acquisition processes are inadequate to deliver the capabilities necessary to outpace the fast-evolving UAS threat. We can no longer afford multi-year requirements development followed by lengthy science and technology experimentation cycles. Government and industry must work together to develop and field new agile counter-UAS programs, and pair these programs with key authorities designed to protect critical infrastructure.

Effective solutions require affordable, open, and adaptable technologies rather than high-cost, proprietary systems. Operational clarity and streamlined authorities are essential for establishing guidelines for UAS detection and defeat within domestic air space. Government and industry partnership will benefit all parties, maximizing innovative and delivering cost-effective solutions.

Solutions must be tailored to meet the unique demands of countering UAS threats. To succeed, we need acquisition reform—but we also need operational clarity. Homeland security stakeholders must work together to establish operational directives that define authorities for UAS detection, identification, and defeat in domestic air space and enable responsible action under clearly-defined legal and safety parameters.

The rapid increase in UAS lethality—as demonstrated in the Ukraine conflict, where drones now cause the majority of casualties—serves as a stark warning. Our traditional defenses and authorities have not kept pace, and we must act swiftly to prevent similar threats against our infrastructure and population.

OPPORTUNITIES

U.S.-based defense innovators are developing promising systems to detect, track, and defeat UAS threats. Soft-kill techniques, such as jamming or radio frequency (RF) manipulation, have dominated this space in the past 5 years. In an effort to combat these defensive tactics, adversaries increasingly employ drones guided by fiber optics, preprogrammed autonomy, various frequency bands, or cellular signals. A few systems, like ours at AV, have capabilities against GPS. The existing authorities make it difficult to utilize these advanced technologies, so we are expanding our ability to counter peer threat capable systems. In parallel, we must continue the development of hard-kill solutions—systems that physically destroy or disable drones.

As has been heard in testimony before other House committees, the President's budget requests critically-needed investments in drone technologies and policy

changes to improve acquisition and production of drone systems, at scale. The Government is poised to be able to take advantage of fast-moving private-sector innovation to field low-cost, attritable, kinetic, and non-kinetic UAS and counter-UAS systems.

Detection technologies, directed energy (laser) and kinetic defeat capabilities offer a promising path forward. The U.S. Army, for example, has demonstrated the effectiveness of high-energy laser systems deliver hard-kill effects with minimal collateral damage. When combined with acoustic sensors, passive radar, and software-defined radio receivers, this creates an integrated drone shield that can be safely deployed in mixed civilian environments focused today on small and medium-sized UAS at close range. Kinetic alternatives, like the Army's Next Generation Counter-UAS Missile, complement directed energy solutions, allowing affordable defense at greater range, elevation, and weather scenarios, though the employment of these systems would be limited in accordance with the sensitivity of the protected infrastructure and public safety requirements. Kinetic solutions are more effective against large UAS, which have been used extensively in Ukraine and the Middle East. These offerings provide alternatives to the unsustainable practice currently employed of shooting down low-cost drones with multi-million-dollar weapons systems, which are expended upon use and difficult to replace.

These technologies are ready, but they require strong demand signals, enabling policies, and streamlined authorities to mature and scale. Without decisive action, the United States risks trailing our adversaries' rapid innovations. We need expanded authorities for UAS defeat operations inside U.S. borders, clear operational doctrines, and funding structures that reward responsiveness. With additional authorities and funding, the defense industrial base can meet the needs of the country. Affordable, attritable platforms at mass are transforming the way in which we fight and are rapidly evolving in a way that necessitates we take advantage of solutions available today, both custom and commercial. We commend the DoD's continued efforts to eliminate overly bureaucratic processes and fund the fielding of systems across all domains.

AV, alongside other forward-leaning, innovative U.S. companies, stands ready to meet this challenge. However, policy inertia and acquisition drag—not technology—remain our most significant obstacles. It is encouraging to see agencies like DoD, DHS, and Members of Congress and committees like yours begin to take steps to rectify the issues we face today. All parties understand that we must act now to prevent foreign battlefield experiences from becoming domestic tragedies.

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

Mr. GIMENEZ. Thank you, Mr. Hutton.

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

STATEMENT OF TOM WALKER, FOUNDER AND CEO, DRONEUP, LLC

Mr. WALKER. Chairman Gimenez, Ranking Member McIver, and Members of the committee, thank you again for the opportunity to testify this morning.

My name is Tom Walker. I am the CEO of DroneUp and a former U.S. Naval officer, and I lead one of the Nation's top drone technology companies.

Over the past decade, I've been proud to play a part in the evolution of uncrewed systems from novelty tools to essential elements of our critical infrastructure.

Today, we've all seen that these systems are also emerging as national security threats.

DroneUp has operated one of the most significant drone services operations in the United States with tens of thousands of operators. We also built one of the most extensive drone delivery networks in the world.

Through our work with the FAA and the national defense agencies, we have gained direct operational insight into both the extraordinary promise and the real dangers of drone technology.

Today, our air space faces an urgent threat. In the first quarter of 2025 alone, the FAA recorded more than 400 illegal drone incursions over U.S. airports, representing a 25 percent increase over the same period last year. The military documented or reported 350 unauthorized flights over more than a hundred bases.

These are not isolated events. They are growing, sustained, and increasingly malicious.

In one case, persistent hostile drone activity forced the relocation of F–22 Raptors at Langley Air Force Base in Virginia. Despite weeks of investigation by the Pentagon, the FBI, and NASA, the operators were never identified.

As a veteran, it scares the hell out of me to imagine if something like that had happened during Operation Midnight Hammer.

Just 2 weeks ago, as the Ranking Member mentioned, during high-intensity search-and-rescue operations amid the July 4 flash floods in Texas, a privately-operated drone struck a rescue helicopter over Kerr County forcing it to land and taking it out of service while dozens were still missing.

Fortunately, no one was injured in the accident. However, the incident could have had very different outcomes. It's the latest reminder that these are not hypothetical threats. They are happening now in active emergency zones and putting lives at risk.

These threats now affect nearly every sector that is exposed to air space misuse, including commercial aviation, critical infrastructure, prisons, and public events. Drones have recently collided with manned aircraft and in some cases have grounded emergency response efforts.

Criminals have used drones to drop contraband into correctional facilities. They have conducted surveillance on energy facilities and seaports.

This is no longer theoretical. The systems meant to stop this are simply not up to the task.

The root problem is simple: We do not have an integrated national framework for drone oversight. The system we were promised still does not exist.

We rely on fragmented tools. We rely on unconnected sensors. We rely on outdated approval processes. This creates blind spots. It slows response time and it leaves critical infrastructure exposed.

But the solutions are within reach. The technology to keep Americans safe exists today.

We must mandate a national real-time flight information exchange. We need a low altitude air space coordination system that provides law enforcement, regulators, and commercial operators with a real-time view of what is flying, where it is, and its intentions.

We must unify all flight authorizations into a single secure process. We must bind pilot, drone, and mission data together, using cryptographic credentials to prevent spoofing.

All aircraft, manned and unmanned, should electronically broadcast their position to reduce collision risk and remain visible in our air space.

Remote ID signals must be authenticated and protected from spoofing. Detection systems, such as radar, RF, and acoustic tools, must be fused into a single integrated surveillance picture.

The FAA should publish national mission priority tables. This must digitally be enforced by the authorization system so that emergency and critical flights are automatically prioritized.

America must equip and empower local law enforcement by expanding its counter-UAS authority. Today, only a handful of Federal agencies are authorized to act against rogue drones. That must change before the current authority sunsets in September.

This is no longer a concern for the future. It's a present-day crisis. Each delay increases our exposure to a serious event. The technology is ready. What we need now is clear direction and decisive action.

I stand ready to assist the committee in protecting our national air space and ensuring the safe, responsible growth of uncrewed systems in the United States.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Walker follows:]

PREPARED STATEMENT OF TOM WALKER

JULY 8, 2025

INTRODUCTION AND PURPOSE

Chairman Gimenez, Ranking Member McIver, and Members of the committee: I am Tom Walker, chief executive officer of DroneUp and a former U.S. naval officer. Throughout my career, from military service to leading one of the Nation's largest uncrewed aviation networks, I have witnessed the rapid evolution of drone technology, both in its ability to serve the public and in the emerging risks it poses to national security.

My written testimony provides operational data and first-hand insights from thousands of commercial drone missions conducted across the United States. These missions have revealed consistent vulnerabilities in our air space and infrastructure that warrant urgent attention from the Federal Government.

I will also outline practical measures that government and industry can take together to close these gaps, improve air space coordination, and reduce the risks posed by uncrewed systems.

I appreciate the committee's leadership on this issue and stand ready to support efforts to ensure the safety, security, and scalability of U.S. air space.

BACKGROUND AND QUALIFICATIONS

DroneUp was founded in 2016 to scale drone services nationwide. We built what became the world's largest drone services network, activating tens of thousands of independent drone pilots nationwide.

We subsequently launched the largest drone delivery operation in the country at that time, with the capacity to serve nearly 4 million households through partnerships with major retailers and State governments.

As part of that effort, we operated 34 drone hubs in 6 States, including Chairman Gimenez's home State of Florida. We obtained FAA Part 135 Air Carrier Certification and gained first-hand insight into both the operational potential and the technical limitations of drone systems at scale.

As our operations expanded, it became clear that the most significant constraint was not aircraft performance or logistics. The limiting factor was the absence of a technological foundation to safely integrate uncrewed systems into national air space. Ensuring future aviation safety, protecting critical infrastructure, and maintaining safe separation between crewed and uncrewed aircraft requires a systems-level solution.

Today, DroneUp focuses on integrating autonomous air space using AI-enabled technology. Our platform enables real-time deconfliction, autonomous flight coordination, and persistent situational awareness in dynamic and high-risk environments. We collaborate directly with Federal regulators, defense agencies, and commercial operators to close security and operational gaps that traditional aviation systems were never designed to address.

This perspective is grounded in real-world operational experience and technical development. It reflects what we are already observing in the field and what must now be done to protect the air space.

OVERVIEW OF THE THREAT LANDSCAPE

As of mid-2025, the United States is facing a sharp escalation in drone-related threats across aviation, infrastructure, and national security. In the first quarter of 2025 alone, the FAA recorded 411 illegal drone incursions near U.S. airports, a 25.6 percent increase over the same period in 2024 (FAA).

Separately, U.S. Northern Command documented over 350 unauthorized drone flights across more than 100 military installations in 2024 (Fox News).

These are not isolated incidents. They are active, sustained, and growing. They disrupt flight operations, interfere with emergency services, and expose vulnerabilities at military and civilian facilities nationwide.

This is not a domestic problem alone. Internationally, drones have shut down major airports, penetrated secure sites, and been used for espionage, sabotage, and targeted attacks. When drone activity shut down London's Gatwick Airport for 33 hours in 2018, it disrupted 1,000 flights and stranded over 140,000 passengers (BBC). That type of disruption is no longer hypothetical here. It is beginning to happen on U.S. soil.

The threat is real, immediate, and growing faster than our ability to contain it.

THREATS TO AVIATION

Drones now pose a direct and rising risk to manned aviation in the United States. In 2024, they accounted for nearly two-thirds of all reported near-mid-air collisions at the Nation's 30 busiest airports, according to analysis by the Associated Press and NASA's Aviation Safety Reporting System (AP News, The Sun).

Pilots have reported drones within hundreds of feet of commercial aircraft during takeoff and landing:

- A quadcopter flew within 300 feet of a jetliner's cockpit on approach to San Francisco International (AP News)
- A drone was observed at 4,000 feet near Miami International
- At Newark Liberty, a drone came within 50 feet of a departing jet's wing.

The FAA continues to receive over 100 drone sighting reports every month near U.S. airports (FAA).

The trend is accelerating, and these are not all near misses. In January 2023, an F–16 fighter jet collided midair with a drone during a training mission over Arizona (AZFamily). In January 2025, a drone struck a Los Angeles County firefighting aircraft during an emergency evacuation, tearing a 6-foot hole in the wing and grounding the aircraft while 192,000 residents were under evacuation orders (ABC7, AP).

The threat is global. In September 2023, a Virgin Atlantic Boeing 787 carrying 264 passengers narrowly avoided a drone collision just after takeoff from Heathrow Airport. U.K. aviation authorities described it as one of the closest calls on record (D-Fend Solutions).

Many of these drones are too small to appear on radar and are often operated by individuals who may not be visible to authorities. Without stronger detection systems, improved coordination, and apparent enforcement authority, the risk to commercial and emergency aviation will continue to grow.

THREATS TO CRITICAL INFRASTRUCTURE

Military Installations

Drone incursions into U.S. military air space have reached unprecedented levels. In December 2023, Langley Air Force Base in Virginia experienced 17 consecutive nights of drone overflights. Witnesses described formations as large as 20 feet long, traveling at 100 miles per hour, and reaching altitudes of 3,000 to 4,000 feet (Task & Purpose). The incident forced the relocation of F–22 Raptor aircraft and the suspension of training operations. Despite weeks of investigation by the Pentagon, FBI and NASA, the drone operators were never identified.

In December 2024, Wright-Patterson Air Force Base was forced to close its air space for 4 hours due to heavy UAS activity. Controllers reported multiple unidentified drones operating over the facility (CNN, The War Zone).

These are not hobbyist drones. These are sustained, strategic incursions targeting sensitive national security infrastructure.

Energy Infrastructure

In 2024, over 13,000 drone incursions were detected at U.S. power generation sites. Analysts estimate that 60 new vulnerability points are added to the grid every

day (E&E News, Dedrone). The Department of Homeland Security has warned that extremist actors and foreign adversaries have considered using drones for surveillance or sabotage.

In January 2024, the Cybersecurity and Infrastructure Security Agency and the FBI issued a joint advisory warning that Chinese-manufactured drones operating in the U.S. energy and telecommunications sectors could expose sensitive data to foreign access (CISA).

Prisons

Drones are now a standard tool for delivering contraband into U.S. prisons. From 2023 to 2024, Georgia reported 774 drone sightings at State correctional facilities. Of these, 720 involved contraband drops, including drugs, weapons, and cell phones. The incidents led to over 540 felony arrests. At Washington State Prison alone, authorities intercepted 21 drone drops in 1 year, arresting more than 40 individuals linked to smuggling operations (WGXA News).

Public Events

In 2023, NFL stadiums reported 2,845 unauthorized drone incursions, up from just 67 in 2018, a 4,145 percent increase (Reuters). The NFL, Department of Justice, and FBI have all called on Congress to expand detection and mitigation authority to protect public events.

Ports and Maritime Infrastructure

America's maritime transportation system underpins more than $5.4 trillion in economic activity and carries over three-quarters of all U.S. trade, according to the 2023 Cyberspace Solarium Commission and independent StateScoop reporting. (cybersolarium.org, Statescoop.com)

Yet ports remain attractive, under-protected targets. The Port of Los Angeles blocked roughly 60 million attempted cyber-intrusions every month in 2023, up from 7 million in 2014, its chief information security officer told trade press and security researchers. (ajot.com, amu.apus.edu)

At the same time, the U.S. Coast Guard warns that unauthorized drone flights over sensitive maritime facilities have become "a common occurrence," and that most local authorities still lack the equipment and legal authority to detect or interdict them. (hstoday.us)

These low-cost aircraft can hover above container stacks, record ship movements, and capture other line-of-sight intelligence that traditional perimeter systems cannot block, exposing a critical gap between the economic value of U.S. ports and the security resources dedicated to protecting them.

CONCLUSION: A GROWING GAP BETWEEN THREAT AND RESPONSE

These incidents are not anomalies. They reflect an accelerating pattern. Drone technology is becoming faster, cheaper, and easier to operate, while our detection systems, legal authorities, and response capabilities have not kept pace. From airliners and emergency aircraft to power grids, prisons, and ports, drones are exposing fundamental operational gaps.

If these vulnerabilities are not addressed with urgency and coordination, it is not a matter of if they will be exploited, but when and with what consequence.

THE SYSTEM WE WERE PROMISED STILL DOESN'T EXIST, AND THE GAP IS DANGEROUS

By 2017, NASA's UTM trials had demonstrated that data-driven services, rather than radio calls, could safely manage low-altitude drones. The industry told Congress that a nationwide system was imminent. Every drone would file a digital plan, receive near-instant clearance, and broadcast a trusted ID while shielding crewed aircraft and sensitive air space.

Eight years on, that promise remains unfulfilled. LAANC automates only the simplest flights; Remote-ID is little more than a broadcast license plate; and the architecture intended to weave authorization, intent, surveillance, and enforcement into a single safety net stalled at the prototype stage. The low-altitude NAS is a patchwork of manual waivers, siloed registries, partial awareness, and policy-only defenses.

Nine critical gaps keep the system fragmented:

1. Patchwork Authorization.—Anything beyond basic flights slides into slow waivers; approval pipelines don't share live pilot, aircraft, or risk data, so regulators default to broad caps no one can enforce.

2. Fragmented Identity.—Pilot certificates, hull IDs, Authorizations, and Restrictions all live in different databases. Nothing cryptographically binds drone + pilot + mission.

3. No Live Intent Ledger.—While each DSS can expose only minimal "need-to-know" metadata, each USS keeps its complete plans private. Multiple DSSs can overlap but federate only on a best-effort handshake, with no cryptographic trust anchor or shared governance in place. The result: no authoritative, real-time ledger of intent, leaving controllers, law enforcement, and defense without a complete situational picture or conformance guarantee.

4. Prototype-level UTM Functions.—While basic constraint ingestion has been proven, functions such as collaborative detect-and-avoid, demand/capacity balancing, and dynamic rerouting remain at the prototype stage, even as low-altitude drone activity continues to rise faster than the supporting infrastructure can keep pace.

5. Policy-only Protection.—Flight rules, TFRs, and NOTAMs depend on voluntary compliance. The 2018 Gatwick shutdown demonstrated how quickly policy can fail when authorities can't verify or neutralize a rogue drone. The recent withdrawal of manufacturer geofences further widens the exposure.

6. Thin Cooperative Detection.—Remote-ID has a limited range, can be spoofed, and has experienced slow adoption; significant gaps exist in conformance validation and law enforcement's ability to respond.

7. Invisible Manned Traffic.—ADS–B Out is mandatory only in controlled cores. Below 10,000 ft or outside Mode C veils, numerous helicopters and general aviation aircraft fly electronically dark. Drones must either hire human spotters or stay grounded, while manned pilots receive no warning, creating an asymmetric blind spot that endangers safety and national security.

8. Siloed Non-cooperative Sensors.—Radar, RF, acoustic, and EO/IR feeds terminate in siloed consoles. Without a consolidated fusion layer that de-duplicates tracks, tags provenance, and applies confidence scores, agencies lack an authoritative air picture; low-signature threats slip through the seams while false alarms drain resources.

9. Minimal Enforcement Tools.—Many agencies lack the resources, statutory authority, or training to act; penalties rarely deter non-compliance.

These gaps compound: the labyrinthine nature of authorizations, weak identity, a missing intent ledger, and endless prototype tests and deployments have left the NAS blind. Policy-only protection and scant enforcement embed risk; asymmetric conspicuity and unfused sensors hamper both safety and security. Domestic incidents, from prison contraband drops to critical-infrastructure overflights, are accelerating, and foreign actors already field swarm-scale, AI-directed drone operations that would overwhelm today's fragmented defenses.

Without a fully digital, interoperable, security-grade low-altitude traffic management and security backbone, we risk ceding safety, commerce, and strategic credibility. Closing these gaps requires a cohesive national program. One that unifies real-time authorization and intent data, provides universal e-conspicuity for every aircraft, fuses cooperative and non-cooperative sensor feeds, and ensures adequately funded enforcement and training, so that every flight is known, every risk is quantified, and every violation is actionable.

BUILDING A SAFE, TRUSTED, AND SCALABLE LOW-ALTITUDE AIR SPACE

What we need today is not theoretical. It is practical, achievable, and urgent. The foundation is simple. If something is in the sky, we should know what it is, who is operating it, whether it belongs there, and how to respond if it does not.

ESTABLISH A NATIONAL LOW-ALTITUDE INFORMATION & FLIGHT EXCHANGE

The exchange will provide every UAS Service Supplier and Government stakeholder with a live, sub-second view of low-altitude air space by requiring them to publish their flight data to, and subscribe to, a common event bus protected by role-based access control. An immutable, cryptographically-signed ledger will preserve each transaction, enabling regulators, first responders, and counter-UAS systems to verify provenance and reconstruct events with forensic certainty.

DEPLOY A UNIFIED FLIGHT-AUTHORIZATION SERVICE

This service will replace disparate grids, waivers, and letters of authorization with a single standards-based API. Operators will submit an Operational Intent that describes their mission and objectives. The service will automatically validate air space status, aircraft performance, crew credentials, and relevant exemptions, and then issue a digitally-signed authorization token. The token will be broadcast via Remote-ID during flight and stored in the National Low-Altitude Information and Flight Exchange, providing field personnel with instant compliance checks and enabling the FAA with a tunable, permission-verified control point for all mission types.

MANDATE DIGITAL CREDENTIALS & BINDING

Verifiable credentials will cryptographically bind pilot, aircraft, flight plan, and authorizations. Any mismatch or change in authorization will block take-off and trigger immediate alerts. Public-safety officers will resolve a Remote-ID signal to a licensed operator with one query, and insurers will rely on tamper-evident evidence after an incident.

REQUIRE UNIVERSAL ELECTRONIC CONSPICUITY

All crewed and uncrewed aircraft will transmit a verifiable position signal using on-board equipment or low-power beacons. Making every aircraft electronically visible balances the see-and-avoid burden and enables safe, scalable drone operations nationwide.

IMPLEMENT NETWORK REMOTE-ID & NON-REPUDIATION

Add a compact cryptographic signature to every Remote-ID packet, broadcast or on-line, so the Unified Flight Authorization Service, public-safety observers, and counter-UAS sensors can verify authenticity within milliseconds. Spoofed or replayed identifiers will be flagged instantly, while genuine packets will flow unchanged into the National Low-Altitude Information & Flight Exchange as tamper-proof evidence. Every legitimate drone in U.S. air space will thus carry a verifiable, non-repudiable identity, providing regulators, integrators, and first responders with the cryptographic certainty needed to automate trust decisions at machine speed.

ADOPT A MISSION-PRIORITY RULES ENGINE

Embed a five-tier priority framework directly in the authorization service so emergency, public-safety, and critical-infrastructure flights automatically outrank commercial and recreational missions. The engine will eliminate manual deconfliction and restore predictability for time-sensitive operations.

BUILD A SENSOR-FUSION BACKBONE FOR LOW-ALTITUDE SURVEILLANCE

Fuse cooperative tracks from the National Low-Altitude Information & Flight Exchange with radar, RF, acoustic, and electro-optical detections provided by Government and commercial sources. Privacy controls will permit graduated data disclosure, ensuring that all authorized users, from airport towers to local law enforcement, use the same trusted, continuously-updated common operating picture.

LAUNCH A FRIEND-OR-FOE API

Provide authorized sensors and effectors with a one-call verdict: COMPLIANT, UNKNOWN, or HOSTILE, plus confidence and priority metadata. This API will shorten decision cycles, reduce friendly-fire risk, and log every query for after-action accountability.

OPERATE A FLIGHT-RESTRICTED-AREA SERVICE

Publish a single, near-real-time catalog of restricted air space, § 2209 critical-infrastructure sites, stadium Temporary Flight Restrictions, wildfire boxes, VIP security rings, and temporary counter-UAS volumes, and push updates digitally within seconds. The authorization service will validate the current catalog during planning and periodically in flight. If a change is detected, onboard logic will force a reroute or a safe landing, delivering geofence-like protection in a standardized, manufacturer-agnostic format.

FUND A LOCAL ENFORCEMENT EQUIP-AND-TRAIN PROGRAM

Supply State, local, Tribal, and territorial agencies with multi-band Remote-ID receivers tied into the National Low-Altitude Information & Flight Exchange, a Friend-or-Foe-enabled mobile application, and concise on-line training. Statutory amendments will authorize certified officers to order landings or seize non-compliant aircraft, transforming Federal data streams into actionable local enforcement.

START A VEHICLE-TO-VEHICLE SPECTRUM & STANDARDS INITIATIVE

Kick off a technical and regulatory effort to identify and allocate low-latency spectrum for direct detect-and-avoid messaging between crewed and uncrewed aircraft, while deferring any equipage mandate until the Unified Flight-Authorization Service and Universal Electronic Conspicuity have operated long enough to reveal any remaining mid-air-collision risk.

WHY TIME IS CRITICAL

The pace of the drone threat is outstripping our national response. What was once a future-looking concern is now a present and growing danger. The volume, complexity, and frequency of drone-related incidents are rising across every major sector: commercial aviation, military installations, public infrastructure, law enforcement operations, and emergency services. Each passing month adds to the evidence that we are operating in a risk environment that is evolving faster than our laws, technologies, and authorities can keep up.

This urgency is not abstract. It is measurable in hard numbers and operational strain. In the first quarter of 2025 alone, drone incursions near airports increased by more than 25 percent compared to the previous year. Security officials at military bases are now forced to treat drone sightings as recurring operational threats rather than one-off anomalies. Emergency response aircraft have been grounded mid-mission. Correctional facilities and utility providers are managing not theoretical vulnerabilities, but routine air space violations.

What makes the current threat especially urgent is that many of the most critical policy tools to address it already exist on paper, but have not been implemented. For example, FAA Section 2209, mandated initially in 2016, was intended to create a process for restricting drone flights over critical infrastructure. Nearly 9 years later, the rule remains unfinalized, leaving power plants, refineries, and other sensitive sites without the reliable Federal protection they need.

Similarly, the FAA's long-awaited rule to enable beyond visual line-of-sight (BVLOS) drone operations remains delayed. This rule is essential not only for commercial expansion but also for ensuring the safe and scalable use of drones in emergency response and infrastructure monitoring. Its continued absence has created both operational inefficiencies and potential safety risks.

Most concerning is the limited authority for detecting and neutralizing rogue drones. As of today, only a handful of Federal agencies have narrowly defined counter-UAS mitigation authority. State and local law enforcement, as well as most infrastructure operators, remain legally barred from using even basic mitigation tools. Bipartisan proposals to expand this authority have been repeatedly drafted, but Congress has yet to act. If the current Federal authority sunsets in September 2025 as scheduled, no agency, Federal or local, will have a clear legal ability to respond to a malicious drone in real time.

We are approaching a point where the probability of a serious incident, such as a downed aircraft, a disrupted power grid, or a mass evacuation triggered by an air space breach, is no longer low. Without coordinated action, the current patchwork of regulations and capabilities will leave critical gaps that adversaries, criminals, or careless actors can continue to exploit.

The United States has the technological capacity to lead in the safe and secure integration of drones. But every delay in closing these policy and infrastructure gaps increases the risk to public safety and national security. Time is not neutral. Inaction allows the threat to mature, while preparedness becomes more difficult and costly.

We are not sounding the alarm in anticipation of a future crisis. We are responding to the reality that the crisis has already begun. The question before us is how quickly we choose to act.

CONCLUSION AND CALL TO ACTION

The vulnerabilities outlined in this testimony are not theoretical; they are real and present a significant risk. They are documented, active, and growing. The threats posed by uncrewed aerial systems to aviation safety, critical infrastructure, and national security have increased in frequency, complexity, and impact. At the same time, the systems designed to detect, identify, authorize, and respond to these threats remain fragmented, underdeveloped, and in many cases unenforced.

The foundational technologies required to close these gaps are already available. Real-time air space coordination, digital flight authorization, cryptographically-verifiable credentials, secure identity broadcasts, and integrated sensor fusion are not experimental. These capabilities have been demonstrated in operational environments and validated through collaboration between Government and industry. What remains is the directive to implement them at scale.

To that end, I respectfully submit the following priorities for immediate Congressional action:

1. Mandate the establishment of a national real-time low-altitude air space coordination framework. This system must integrate flight intent, identity, and enforcement data into a single operational platform.

2. Require digital credentialing that binds pilots, aircraft, missions, and authorizations. This will enable instant validation of lawful flights and allow for automated detection of non-compliant activity.
3. Implement a universal electronic conspicuity requirement for all crewed and uncrewed aircraft operating below 18,000 feet. This is essential for ensuring visibility and reducing the risk of mid-air collisions.
4. Finalize FAA Section 2209 and direct the creation of a Federal flight-restriction service. This service must provide a machine-readable feed that all drones and autopilot systems consult before and during flight.
5. Expand counter-UAS detection and mitigation authority to qualified State, local, Tribal, and territorial agencies. Oversight and safeguards must be in place, but these agencies need the authority to act.
6. Fund and deploy a local law enforcement equip-and-train program. This program must provide officers with the tools, training, and legal clarity to verify and respond to drone threats in the field.
7. Require the FAA to implement a unified flight authorization service. This service should support all drone operations through a single digital process from request to real-time verification.

Each of these actions addresses a core structural weakness that has allowed unregulated drone activity to outpace national preparedness. These are not isolated or speculative risks. They are recurring incidents that have grounded emergency aircraft, disrupted commercial aviation, penetrated military air space, and exposed key infrastructure to surveillance and interference.

The time line for addressing these issues is urgent. As the pace of drone innovation continues to increase, so does the risk of a high-consequence event. The United States cannot afford to treat low-altitude air space as an ungoverned or optional domain. It must be protected with the same level of accountability and structure applied to every other mode of transportation that affects public safety and national defense.

Congress has both the authority and the responsibility to ensure this system is put in place. The tools are ready. The risks are known. The solution is feasible. What is needed now is coordinated direction and the will to act.

I thank the committee for the opportunity to provide this written testimony. I stand ready to support any effort that will help secure the national air space system and enable the safe, scalable, and responsible integration of uncrewed aircraft systems in the United States.

Mr. GIMENEZ. Thank you, Mr. Walker.

I now recognize Mr. Feddersen for 5 minutes to summarize his opening statements.

STATEMENT OF BRETT FEDDERSEN, VICE PRESIDENT, STRATEGY AND GOVERNMENT AFFAIRS, D-FEND SOLUTIONS

Mr. FEDDERSEN. Good morning, Chairman Gimenez, Ranking Member McIver, and distinguished Members of the subcommittee. Thank you for the opportunity to testify before you on matters of critical importance to the national security and public safety of our country and our citizens.

My name is Brett Feddersen. I am the vice president of strategy and government affairs at D-Fend Solutions, the leading counter-drone manufacturer of radio frequency cyber takeover solutions for drone threats, both domestically and internationally.

I also serve as the chair of the Security Industry Association's drone security subcommittee and have been working on the drone and counter-drone problem set since 2008. During my time in the military, as a Federal civilian, and in the private sector, we've seen this problem grow.

Today, I hope to help the subcommittee better understand how overseas drone operations are transforming domestic risk vectors, the status of the U.S. capabilities and legal frameworks, and offer targeted recommendations for Congress to bolster detection, inter-

diction, and resilience against drone-borne threats in the United States homeland.

Drones have transitioned from niche reconnaissance tools to central components of modern warfare. Their wide availability, small size, low cost, and modular payloads make them attractive for intelligence, surveillance, and reconnaissance, as well as destruction of critical infrastructure and effective delivery of ordnance.

In conflicts outside the United States, inexpensive commercially-available drones and do-it-yourself drones have become the weapon of choice.

Alarmingly, these same drones are flown across the United States every day. There are over 1 million drones registered in the United States according to the FAA, and that number is predicted to grow to 2.7 million by 2027.

The weaponization of private drones in the United States is also a significant and growing concern. While drones have been beneficial applications with public safety and various industries, their potential misuse, especially when armed, poses challenges for law enforcement and national security.

Battlefield tactics, techniques, and procedures for drones have proliferated through the internet and are ready to be used today.

During my time at the FAA, we received several videos and briefings showcasing drones outfitted with chainsaws, flamethrowers, firearms, and makeshift chemical dispensers.

Just weeks ago, the world witnessed a historic shift in small drone warfare. Ukraine's planning and execution of Operation Spiderweb has rewritten the rule book on drone threats: distance, cost, and autonomy no longer constraining our adversaries.

The audacious plan involved Ukraine striking Russian air bases up to 3,100 miles from the battlefield using small commercially-available AI-enabled drones.

For context, this is equivalent to conducting an attack by drone in Los Angeles, California, from your home in Cape Cod, Massachusetts.

This attack demonstrates the capability to build and deploy do-it-yourself drones at scale and at distance, accurately delivering ordnance to create strategic impact and fast destruction of significant assets.

An attack like this can be prevented today using current safe and effective counter-drone technology, such as RF cyber takeover technology which can detect, track, identify, and take control of the drone, then landing it safely when and where law enforcement or security want it to.

This type of technology is legal and safe to use. It does not violate privacy laws or Fourth Amendment protections. And it does not implicate Federal wiretap or pen trap statutes or regulations.

According to the FAA data and previous DOD testimony, drone incursions have steadily increased since the establishment of the Federal counter-drone authorities in 2018. That 5-year pilot program is now in its seventh year.

First responders report that drones are tailing SWAT teams, dropping contraband into prisons, spying on neighbors, and hovering over chemical plants.

While the threat is local, the legal tools remain predominantly Federal in nature.

DHS, DOJ, the security industry, State and local law enforcement, Tribal and territorial law enforcement agencies, along with trained security professionals, have repeatedly urged Congress to expand authorities to enable air domain awareness and drone protection in American communities and over our critical infrastructure.

Unfortunately, those requests have not resulted in any expanded new authorities and limited authorities since 2018 have been periodically renewed only for short periods of time, creating uncertainty for law enforcement and the industry.

To summarize, drone warfare abroad has evolved rapidly over the past decade. Regrettably, U.S. legislation, regulation, and policy has not. Today, we should acknowledge the topic of drone threats in our homeland is neither timely nor new.

What we can say is that the threat is real, the United States is vulnerable, and that without bold and immediate legislative action the American public will remain unprotected from a drone attack.

The industry agrees an attack is only a matter of time. It is not a matter of if it will happen.

I strongly urge the subcommittee and the full committee to take immediate action in meaningful bipartisan legislation.

The industry, public safety professionals, and American public are calling for 3 simple actions that can be taken now to make Americans and our skies safer.

Expand authorities to State and local law enforcement and trained security professionals guarding our critical infrastructure.

Develop and implement a counter-UAS training program using a Federally-accredited curriculum.

Provide dedicated funding programs that enable critical infrastructure operators to procure, train, deploy, and operate counter-UAS systems.

Thank you for your leadership and the opportunity to appear before you. I look forward to taking your questions.

[The prepared statement of Mr. Feddersen follows:]

PREPARED STATEMENT OF BRETT FEDDERSEN

JULY 8, 2025

INTRODUCTION

Chairmen Gimenez and Green, Ranking Members McIver and Thompson, and distinguished Members of the subcommittee, thank you for the opportunity to testify before you on matters critically important to the national security and public safety of our country and its citizens.

My name is Brett Feddersen, and I am the vice president of strategy and government affairs at D-Fend Solutions, the leading counter-drone manufacturer of radio frequency (RF)-cyber takeover solutions for the drone threat, both overseas and in the United States. I also serve as the chair of the Security Industry Association's (SIA) drone security subcommittee and have been working on the drone and counter-drone problem set since 2008, during my time in the military, as a Federal civilian, and in the private sector. Today, I am honored to appear before the subcommittee representing both D-Fend Solutions and the drone security industry.

Bottom line up front: Drone warfare abroad has evolved rapidly over the past decade, with State and non-State actors fielding drones for surveillance, sabotage, and strikes in theaters from Eastern Europe to the Middle East. Tactics refined in these conflict zones—persistent reconnaissance, weaponized loitering munitions, and satu-

ration swarm attacks—are now manifesting as emerging threats to U.S. homeland and national security.

These threats are here to stay and mean that things like our critical infrastructure—such as power grids, water treatment plants, transportation networks, and communication systems—is increasingly vulnerable to threats from nefarious actors who can exploit drones' capabilities, including surveillance, sabotage, and payload delivery, to conduct physical attacks. Successful drone attacks on critical infrastructure can lead to power outages, transportation disruptions, communication failures, and substantial economic consequences. More concerning is the potential for the loss of human life, for example, a drone using aerosol dispersal or payload delivery over a mass gathering can cause mass panic, causing serious injury or even death to attendees. Confronting this reality requires a proactive and multi-layered homeland defense strategy that includes early detection, safe and effective mitigation technologies, and updated security protocols.

From local football games to open-air shopping centers, large gatherings of Americans are part of our everyday lives and remain incredibly vulnerable to drone-based threats. As the United States prepares to host high-profile, global sporting events like the 2026 FIFA World Cup and the 2028 Olympics, I am grateful that the committee is closely overseeing the threat environment and preparations for these events and is willing to engage in difficult conversations surrounding our real vulnerability and capability gaps.

Today, I hope to help the subcommittee better understand how overseas drone operations are transforming domestic risk vectors, the status of U.S. capabilities and legal frameworks, and offer targeted recommendations for Congress to bolster detection, interdiction, and resilience against drone-borne threats in the United States homeland.

MODERN DRONE WARFARE ABROAD AND AT HOME

Drones have transitioned from niche reconnaissance tools to central components of modern warfare. Their wide availability, small size, low cost, and modular payloads make them attractive for intelligence, surveillance, and reconnaissance missions, as well as the destruction of critical infrastructure and the effective delivery of ordnance.

Just weeks ago, the world witnessed a historic shift in small drone warfare. Ukraine's planning and execution of Operation Spider Web has rewritten the rulebook on drone threats: distance, cost, and autonomy no longer constrain adversary reach. Below are key counter-drone lessons drawn from Ukraine's Operation Spider Web—an audacious campaign in which Ukraine struck Russian airbases up to 5,000 km (3,106 miles) from the front using small, commercial AI-enabled drones. This is farther than driving from New York City to Los Angeles.

Rear Areas Are Not Safe

- Ukraine proved that "strategic depth" offers no immunity: drones launched from deep inside friendly territory reached ostensibly secure Russian airfields, destroying billions of dollars' worth of aircraft. Defenders must extend coverage well beyond the front lines to include logistics hubs, maintenance depots, and forward operating bases.[1]

Defense in Depth—Layer Every Segment

- Traditional point-defense systems (e.g., local radar or a single interceptor battery) were overwhelmed. Operation Spider Web integrated covert logistics, telecom exploitation, and ground infiltration to bypass singular defenses, underscoring the need for a layered approach to counter-drone detection (RF, radar, EO/IR) and mitigation (RF cyber takeover, electronic warfare measures, and directed energy).[2]

Resilience to Jamming and GPS Denial

- Spider Web's drones used dead-reckoning navigation and civilian cellular (SIM-card) links rather than GPS, making them resilient to traditional GNSS jamming. Given this, counter-drone systems should include extensive RF spectrum monitoring, non-GPS-dependent geofencing, and safe mitigation techniques that can detect, take control of, or disrupt alternate control channels.

---

[1] American University, "Ukraine's Operation Spider Web Upended Traditional Rules of War," June 5, 2025. Benjamin Jensen; *chathamhouse.org american.edu*.

[2] Counter-UAS Hub, "Putting Operation Spider's Web in Context," June 20, 2025, Ben Connable; *cuashub.comirregularwarfare.org*.

In conflicts outside the United States, inexpensive, commercially available, and do-it-yourself (DIY) drones have become the weapon of choice. Alarmingly, these same drones are flown across the United States every day. There are over 1 million drones registered with the FAA in the United States—a number that is predicted to grow to 2.7 million by 2027.[3]

The weaponization of private drones in the United States is a significant and growing concern. While drones have beneficial applications in public safety and various industries, their potential for misuse, especially when armed, poses challenges for law enforcement and national security. Battlefield tactics, techniques, and procedures for drones have proliferated through the internet, and the same drones used in combat overseas are available and in use here in the United States.

During my time at the Federal Aviation Administration (FAA), we received several videos and briefings showcasing drones outfitted with chainsaws, flamethrowers, firearms, and makeshift chemical dispersal systems. We have witnessed rocket-propelled grenades (RPG) warheads and grenades being dropped from simple commercial and do-it-yourself (DIY) drones. Additionally, we have seen drones equipped with modified shotguns used to shoot down other drones.

Key Concerns and Examples of Weaponization

- *Potential for Malicious Use*.—Drones can be easily outfitted with various weapons, including firearms, explosives, incendiary devices, or even chemical or biological agents, posing a risk to individuals, critical infrastructure, and Government facilities.
  - *Terrorism*.—Terrorist organizations can adapt and exploit drone technology to target public spaces and infrastructure, potentially magnifying casualties and damage. Cartels operating in Mexico along the U.S. Southern Border are already using weaponized drones to drop munition payloads.
  - *Drone swarms*.—Coordinated attacks utilizing drone swarms can overwhelm traditional defenses and enhance the effectiveness of sabotage operations.
- *Drone Incursions and Modern Espionage*.—There have been numerous drone incursions over sensitive sites, including military bases and critical infrastructure, raising concerns about potential threats. Drones can be used for corporate and foreign espionage, including surveillance of facilities, intimidation through observation, and even cyber attacks by leveraging proximity to networks.
- *Smuggling and Criminal Activity*.—Drones are used by criminals for illegal drug shipments, delivery of contraband into prisons, and counter-surveillance of law enforcement.
- *Privacy Concerns*.—Drones equipped with cameras and other sensors can be used for unauthorized surveillance and invasion of privacy.
- *Interference with Public Events and Aircraft*.—Unauthorized drone flights can disrupt public events and pose a risk to aviation safety, including the potential for collisions with manned aircraft.

Common commercial drones have already been used in attempts to destroy or damage critical infrastructure, and we continue to see variations of weaponized drones attempting to attack the public in the heartland and law enforcement in cities and on the border.

- *2020 Pennsylvania Power Substation Incident*.—A modified drone was discovered outside an electrical substation in Pennsylvania. It was equipped with a copper wire, likely intended to create a short circuit and disrupt power. The drone crashed before reaching its target, but it highlights the potential threat.
- *Attempted Attack in Nashville (2024)*.—A man was arrested in November for planning to use a weapon of mass destruction to attack an energy facility in Nashville. Court documents indicated he planned to use a drone to deliver an explosive.
- *Suspicious Drone Activity Near Energy Sites (2024)*.—In December, multiple energy sites requested temporary flight restrictions due to unusual drone activity in New Jersey, New York, and Maryland. Although the operators weren't identified, this incident reflects the on-going concern about drone threats.

What is Our Current Air Space Protection Posture?

Over the years, drones have evolved from simple weekend toys to sophisticated tools used for smuggling, corporate espionage, and terrorist surveillance. Unfortunately, Federal policies have struggled to keep up with these emerging threats, leaving State, local, Tribal, and territorial (SLTT) law enforcement agencies in a challenging position and their constituents unprotected. These agencies and trained se-

[3] FAA, "Drones by the Numbers," updated April 1, 2025, *https://www.faa.gov/node/54496;* "Drone Operations," Government Accountability Office, *https://www.gao.gov/drone-operations.*

curity professionals are on the front lines protecting critical locations—such as stadiums, power plants, and city skylines—but they face legal restrictions that prevent them from effectively addressing drones that pose a danger to these sites and the American public.

As you know, only a few Federal law enforcement components in the Department of Homeland Security (DHS), Justice (DOJ), and Defense (DoD)—have explicit legal authority under 6 U.S.C. § 124(n) and 10 U.S.C. § 130(i) to detect and mitigate (or stop) illicit drone activities. Other entities, including State and local police departments and trained security professionals, must rely on Federal support or remain powerless, while unidentified drones fly dangerously over parades, concerts, major sporting events, and critical infrastructure. By their own admission, the DOJ and DHS can only respond to less than 1 percent of the thousands of counter-drone operational requests they receive each year.

According to FAA data and previous DoD testimony, drone incursions have steadily increased since the establishment of Federal counter-drone authorities in 2018. First responders report that drones are tailing SWAT teams, dropping contraband into prisons, spying on neighbors, and hovering over chemical plants. While the threat is local, the legal tools remain predominantly Federal in nature.

In 2014, while serving as the National Security Council Director for Aviation Security at the White House, we encountered drone incursions on the White House and Capitol campuses. Subsequently, the interagency met to develop a response plan for these "non-traditional aviation threats." As a result of these efforts, the FAA received Congressional direction to begin testing counter-drone technology systems in 2016. In 2017, the Department of Defense was granted additional authorities. In 2018, Congress authorized a 5-year pilot program for Federal law enforcement as part of the FAA Reauthorization process to provide counter-drone authorities to the Department of Homeland Security (DHS) and the Department of Justice (DOJ). Seven years later, these authorities remain unchanged.

DHS, DOJ, the security industry, and State, local, Tribal, and territorial (SLTT) law enforcement agencies and trained security professionals have repeatedly urged Congress to expand authorities to enable air domain awareness and drone protection in American communities and over our critical infrastructure. Unfortunately, those requests have not resulted in any expanded or new authorities, and the limited authorities from 2018 have been periodically renewed only for short periods of time, creating uncertainty for law enforcement and the industry.

LEGISLATIVE RECOMMENDATIONS AND NEXT STEPS

The President's recent Executive Orders are a good start to address our legislative and regulatory inaction. However, Executive action alone is not a permanent shield—it can be revoked by future administrations or challenged in court. Congress must move now to codify SLTT counter-UAS authorities with the same privacy safeguards and oversight as outlined in President Trump's Executive Orders.

I strongly urge the subcommittee and full committee to take bipartisan legislative action now. The industry, public safety professionals, and the American public are calling for 3 simple actions that can be taken immediately to make Americans and our skies safer.

1. Expand the current 6 U.S.C. § 124(n) detection and mitigation authorities to all SLTT–LE and trained security professionals, safeguarding our critical infrastructure, and amend 49 U.S.C. § 14501 to include an explicit "Counter-UAS Exception," authorizing approved non-Federal entities to employ safe and effective, non-kinetic mitigation under DHS oversight.
2. Develop, implement, and oversee a counter-drone operator training regime, using a Federally-accredited curriculum required for all counter-drone operators using approved mitigation technology; and
3. Provide dedicated funding programs that enable critical infrastructure operators to procure, train, deploy, and operate counter-drone systems deemed safe and effective by the Federal Government.

CONCLUSION

The tactics developed in overseas drone conflicts—such as persistent surveillance, sabotage using payload delivery, loitering munitions, and swarm saturation strikes—are now poised to harm us at home. The increasing number of drone incursions into sensitive air space we've seen in recent years should serve as a loud and distinct alarm bell, warning us of the immediate necessity for deploying safe and effective counter-drone technology to enable rapid response capabilities. While the industry has developed effective detection, identification, and mitigation solutions, challenges such as legal uncertainties, regulatory delays, and funding shortages are

hindering nationwide implementation. To address these issues, Congress should clarify its legal authorities, streamline the approval process, and establish dedicated funding. This will enable U.S. stakeholders to effectively deter and counter drone-related threats before they reach our shores. Now is the time to strengthen our defenses in the skies before tomorrow's headlines report the first successful drone strike on U.S. soil.

Thank you for your leadership and the opportunity to appear before you today. I look forward to answering any questions you may have.

Figure 1
Drone Threat Progression Abroad and in the Homeland

Mr. GIMENEZ. Thank you Mr. Feddersen.

I now recognize Mr. Robbins for 5 minutes to summarize his opening statements.

STATEMENT OF MICHAEL ROBBINS, PRESIDENT AND CEO, ASSOCIATION FOR UNCREWED VEHICLE SYSTEMS INTERNATIONAL

Mr. ROBBINS. Thank you, Chairman Gimenez and Ranking Member McIver and distinguished Members of the subcommittee. It's an honor to be with you here again today and to represent AUVSI and our member companies that are providing solutions in aviation and national security every day.

We're at a pivotal moment in aviation history. Drones and advanced aviation are unlocking tremendous gains for safety, security, technology, and economic opportunity.

These technologies, they're no longer theoretical. They're delivering real-world value today across our economy and for our Armed Forces.

Drones are enhancing public safety, enabling faster emergency response, improving infrastructure inspections, supporting precision agriculture, and expanding package delivery networks.

Across the country, high-rate production facilities are coming online, thousands of skilled manufacturing jobs are being created, and these innovations are expanding access to aviation careers.

But all of that progress and the significant national benefit it represents is at risk today if we fail to address the growing security threats posed by the malicious use of drones.

We've long rightly been focused on aviation safety, but we can no longer afford to ignore the security side of the equation.

I actually entered this industry in direct response to a drone incident. As mentioned by Ranking Member McIver, in December 2018 London's Gatwick Airport, the second-busiest in the United Kingdom, was shut down for nearly 24 hours because of a drone—or possibly multiple drones—spotted near the airfield.

The Government and the airport were paralyzed. Thousands of flights across Europe were canceled or delayed. In the end no one could say with certainty what happened, how to respond, or if the drones were actually ever even there.

In the aftermath of that event, I formed and staffed the Blue Ribbon Task Force on UAS Mitigation at Airports on behalf of AUVSI and the Airports Council International—North America.

Our mission was simple: Make sure a Gatwick-style shutdown never happens in the United States. The task force made dozens of policy recommendations to Congress to help achieve that goal. Unfortunately, most of those have still not been acted upon.

In the years since, we've seen far more serious and frequent drone incursions—in military installations, like, as mentioned, at Langley Air Force Base, at commercial airports and ports and power plants, prisons and disaster response sites, stadiums, and even the White House complex. A Chinese DJI drone was even used in the attempted assassination of President Trump around this time last summer.

We've seen mass confusion over drones—or what some mistakenly thought to be drones—in New Jersey last December, resulting in significant media excitement and very few answers.

We've seen drone warfare evolve at a blistering pace overseas, from Ukraine and the stunning Spiderweb swarm attack last month, to the Middle East and Africa where small, low-cost drones are being used to overwhelm air defenses and carry out coordinated strikes with devastating efficiency.

Despite all of this, U.S. policy hasn't changed, not meaningfully and not at the scale this threat demands.

This is not a technology problem. AUVSI member companies, including the 3 at this witness table with me today, have built and deployed proven, effective solutions for detection, identification, and mitigation of rogue drones.

This is a policy failure, and that failure is putting American lives, infrastructure, and national security at risk.

There is a great deal of finger-pointing whenever unauthorized drones disrupt sensitive air space. But let me be clear: Congress should not be pointing any fingers unless holding up a mirror.

The last expansion of counter-UAS authorities was in 2018, 7 years ago, and the authorities granted are limited and clearly inadequate for addressing the evolving threat. This is an unacceptably long time line.

Furthermore, the lack of progress is unjust to local, State, Tribal, and Federal authorities, including Capitol Police, as well as infrastructure owners and operators, who lack the tools and authorities to do much of anything in a drone disruption situation.

We applaud the Trump administration's Executive Order issued last month restoring American air space sovereignty which begins

to address these challenges. But executive action alone is not enough. Congress must act.

We need legislation that expands detection authority broadly, especially to those responsible for protecting critical infrastructure and mass gatherings, and expands mitigation authority narrowly, with strong training, oversight, and accountability.

We cannot let perfection be the enemy of progress. We need to start chipping away at the problem with urgency and resolve.

Congress can either shape the future with considered proactive legislation or be forced to react to the next crisis with confusion and regret.

Every time a drone is used to spy or disrupt or threaten, it erodes public trust and jeopardizes the life-saving, job-creating, future-defining promise of drone technology.

The time for action is long past. Congress must act to ensure our air space, to secure our air space, empower those on the front line, and ensure that innovation and security are moving forward together.

Thank you, and I very much look forward to your questions.

[The prepared statement of Mr. Robbins follows:]

PREPARED STATEMENT OF MICHAEL ROBBINS

JULY 15, 2025

Chairman Gimenez, Ranking Member McIver, and Members of the subcommittee: Thank you for the opportunity to testify before you today. My name is Michael Robbins, and I am the president and CEO of the Association for Uncrewed Vehicle Systems International (AUVSI), the world's largest nonprofit trade association dedicated to the advancement of uncrewed systems, autonomy, and robotics. AUVSI represents a broad spectrum of stakeholders who are committed to the secure, responsible, and innovative integration of drones and other autonomous technologies into our national air space system and associated infrastructure.

The topic of this hearing could not be timelier. Across the globe, including ongoing conflicts in Ukraine, Africa, and the Middle East, we are witnessing a transformation in modern warfare and at the center of this transformation are uncrewed systems, in particular, unmanned aircraft systems (UAS or drones). Drones transform battlefields because they both extend operational reach as well as reduce the risk to human life. As I have said on a number of occasions, including in recent Congressional testimony, robots don't bleed.[1]

But this hearing is not just about foreign battlefields. What happens abroad is actively shaping the threat landscape here in the United States. Unfortunately, to date, what is happening abroad has not yet meaningfully changed our policy landscape to mitigate these threats. Inexpensive, consumer, and commercial drones that are easily accessible and widely available are being modified to carry out surveillance, cyber disruption, espionage, and kinetic attacks against critical infrastructure. State-sponsored and criminal actors are increasingly looking to these platforms for asymmetric advantages because they are accessible, inexpensive, adaptable, and often undetectable by legacy air defenses. Drone warfare abroad has shown us what's possible, and just as significantly, what's vulnerable.

As the title of today's hearing suggests, the same systems transforming how we move goods, inspect infrastructure, and save lives through public safety operations are also reshaping the threat landscape. Drones are inherently dual-use. Their commercial potential is vast and offers tremendous promise, yet their accessibility and adaptability also make them attractive tools for malicious actors. It is imperative that Federal policy both leverages the benefits of these technologies and mitigates the emerging risks. Innovation and security must advance in lockstep.

U.S. airports, maritime facilities, power plants, prisons, amusement parks, sports stadiums, and even Statehouses have increasingly seen incursions by unauthorized drones. While most are not overt attacks, they are proof points of how porous our

[1] *AUVSI Testifies Before House Aviation Subcommittee on FAA Reauthorization Implementation with Emphasis on Drone & Advanced Air Mobility Regulations—AUVSI.*

defenses remain. Unfortunately, despite the many responsible drone users and operators around our country, especially those operating under Federal Aviation Administration (FAA) rules including Part 107 and Part 135, there are rogue actors looking to utilize these critical life-saving tools for nefarious purposes.

Yet our domestic policy and regulatory framework has not kept pace with the threat. There is no singular Federal authority to counter uncrewed threats, no consistent framework for what technologies can be deployed or by whom, and no mandated reporting of drone incidents that could inform a national picture of risk. Congress has not updated our Nation's UAS detection and mitigation authorities since 2018.[2] Meanwhile, the air space has evolved tremendously, the threat landscape has changed dramatically, and the number of drones operating in the United States has expanded exponentially.

The lack of Federal action and investment has left a dangerous gap in our ability to respond to reckless or nefarious drone activity. Today, only 4 Federal agencies, the Department of Defense (DoD), Department of Homeland Security (DHS), Department of Energy (DOE), and Department of Justice (DOJ), are authorized to detect and mitigate UAS threats, and their authorities are very limited. State and local law enforcement, airport and prison operators, and other critical infrastructure entities are left watching and waiting while unauthorized drones fly overhead.

Today, only a limited number of top-tier events are able to get Federal support and equipment painting a clear picture of the air space. If something catastrophic happens—a drone collision with a passenger aircraft, an attack on a packed stadium, or an intrusion into a sensitive Government facility—finger-pointing will be inevitable. Congress, the White House, FAA, DHS, industry, and local authorities will all scramble to assign blame. But pointing fingers won't prevent a crisis, acting now will.

AUVSI applauds the Trump administration's recent Executive Orders, *Restoring American Airspace Sovereignty*[3] and *Unleashing American Drone Dominance*,[4] that addressed some counter-UAS (c–UAS) related issues and showcased the importance this administration places on drone issues, but Congressional action is still necessary to expand c–UAS authorities.

The threats we're examining today demand a serious and coordinated response, one that strengthens our ability to defend against malicious use of drones while also preserving the critical benefits these technologies bring. Every day, drones support law enforcement, firefighters, energy providers, and emergency response teams in protecting lives and infrastructure. As we enhance our national security posture, it's essential that we also sustain the innovation and trusted uses that serve our communities. Striking that balance is not only possible, but also essential to both our security and our continued progress.

THE DUAL-USE NATURE OF DRONES: A STRATEGIC ASSET AND A TACTICAL THREAT

Events unfolding around the world are not just instructive, they are sounding an alarm we cannot afford to ignore.

In Ukraine, the defense ministry's Operation Spiderweb[5] clearly showcased how swarms of small drones can be used to saturate enemy air space, overwhelm air defense systems, and execute lethal strikes. These low-cost, high-impact platforms are changing the dynamics of warfare, not with brute force, but with agility, coordination, and volume. In the Middle East, Israel has leveraged drones to preemptively disrupt Iranian air defense networks, enhancing the safety and effectiveness of manned and unmanned aerial operations.

These examples demonstrate a common truth: even small, commercially-available drones, when used in a strategic and coordinated manner, can pose serious threats to fixed infrastructure. Ports, bridges, shipping terminals, and maritime chokepoints are all vulnerable to surveillance, sabotage, or disruption by hostile UAS activity. These vulnerabilities do not only exist in active war zones. They exist today, here at home, across the transportation and maritime sectors that support our national economy and security.

In short, the tactics we are witnessing in modern conflict zones are not constrained by geography. The barriers to entry are low, the technology is widely available, and the intent of our adversaries is clear. We must assume that the threat

---

[2] *https://www.auvsi.org/progress-on-domestic-uas-detection-mitigation-is-required-for-public-trust-enabling-drone-regulations/*.

[3] *https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/*.

[4] *https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/*.

[5] *https://en.wikipedia.org/wiki/Operation_Spiderweb*.

is already here, and we must act accordingly to protect the systems and infrastructure that keep this country not only moving, but safe.

DRONES IN TRANSPORTATION AND MARITIME SECURITY: A CRITICAL FORCE MULTIPLIER

Those very same drone systems that can be misused are also being used daily to protect American lives, infrastructure, and supply chains. Across the United States, transportation and maritime authorities are leveraging drones as essential tools for homeland security operations, providing perimeter monitoring, real-time subject tracking, and as part of Drone as First Responder (DFR) public safety programs. These applications allow rapid situational awareness and response to developing threats or incidents.

When used by trusted operators, with secure platforms, drones offer unmatched speed, agility, and visibility. They enable rapid situational awareness, improve officer safety, and shorten response times during high-risk incidents from port intrusions to natural disasters.

In infrastructure management, drones enable safe and cost-effective inspections of bridges, railways, pipelines, ports, runways, and more, tasks that would otherwise require human workers to operate in high-risk, unsafe environments. They provide real-time imaging and data that supports predictive maintenance and operational readiness. A particularly powerful example of the utility of drones came in the aftermath of the Francis Scott Key Bridge collapse in Baltimore, Maryland. Drones were immediately deployed by local and Federal authorities to assist with damage assessment, guide search and rescue teams, and coordinate the emergency response. These operations illustrated the agility, speed, and value of drone systems in supporting critical transportation and maritime missions.

This is the dual-use reality we face. While malicious actors may seek to weaponize this technology, the overwhelming majority of use cases, particularly in public safety and critical infrastructure, are enhancing our ability to respond to threats and protect American lives. As policy makers, it is vital to distinguish between threats and trusted uses, and to ensure that our response to one does not hinder our ability to leverage the other.

NATIONAL SECURITY RISKS FROM PEOPLE'S REPUBLIC OF CHINA (PRC)-MANUFACTURED DRONES

While drones are proving to be essential tools for homeland defense and emergency response, not all systems are created equal, and some represent an active and growing risk. Drones manufactured by companies with ties to the PRC continue to be widely used by public safety and other agencies, even in sensitive infrastructure environments. In some cases, Federal agencies are still using these platforms. This is largely due to the absence of consistent Federal procurement restrictions or guidance and minimal oversight of mandates already enacted into law as part of the American Security Drone Act and other legislation.

The national security implications are stark and well-documented. Numerous assessments by DoD, DHS, and other Federal intelligence agencies have documented how PRC-made drones present unacceptable risks, including unauthorized data collection and transmission to the PRC.

AUVSI has been the tip of the spear in urging the swift implementation of Section 1709 of the Fiscal Year 2025 National Defense Authorization Act (NDAA), which would add the communications equipment and services of PRC drone manufacturers DJI and Autel Robotics (and any of their subsidiaries, affiliates, partners, joint venture entities, or entities with a technology sharing or licensing agreement with a named entity) to the Federal Communications Commission's (FCC) Covered List. This will occur after a relevant national security agency makes a determination on their unacceptable risk to national security, or, on 23 December 2025 as directed by Congress if action is not taken sooner.[6]

Despite these legitimate and documented concerns, many agencies continue to procure and operate PRC platforms due to a lack of consistent Federal policy, market incentives, and clear alternatives. Allowing adversary-linked systems to operate in the heart of our national infrastructure networks is a liability we cannot afford. To defend against emerging threats, we must ensure that the platforms used to secure our infrastructure are not themselves potential vectors for surveillance, sabotage, cyber intrusion, or supply chain warfare.

This is not about cutting off access to drones, it is about ensuring that the platforms used to secure the homeland are not themselves Trojan horses. Allowing systems tied to adversarial governments to operate within our most critical infrastruc-

[6] *Whitepaper: AUVSI Partnership for Drone Competitiveness.*

ture networks is a legitimate threat that we can address through common-sense action.

We cannot effectively defend against surveillance or sabotage if we continue to operate systems that may be compromised from within. Building a trusted, resilient domestic drone ecosystem is not just a competitive advantage, it's a national security necessity here in the United States. Congress must act to accelerate the transition to trusted U.S. and allied systems, by setting clear procurement standards, supporting domestic manufacturing, and incentivizing the adoption of secure platforms.[7]

ADVANCING SECURITY SOLUTIONS AND MARITIME-SPECIFIC APPLICATIONS

Several mature, scalable solutions are already available and in use. Technologies such as Remote Identification (Remote ID), drone detection and tracking systems, and defensive mitigation tools, both kinetic and non-kinetic, have advanced significantly in recent years alone. These tools allow security personnel to identify, assess, and, when authorized, neutralize malicious drone activity.

While much of the public conversation has focused on protecting airports, stadiums, and Federal buildings, our maritime and transportation infrastructure remains significantly under protected.[8] Shipyards, ports, offshore energy platforms, rail crossings, and inland waterways are just as vulnerable to surveillance, sabotage, and disruption; and in many cases, even more difficult to secure due to their geographic scale and open access.

Adaptation of these technologies for maritime domains, including ports, shipyards, and offshore energy infrastructure, is both necessary and feasible. These critical nodes in our logistics and energy networks deserve the same layered protections that are being discussed for airports, stadiums, and Government facilities.

Importantly, these efforts must be guided by clear Federal frameworks that balance security with privacy, protect authorized drone operations, and enable public-private coordination. AUVSI urges Congress to support the deployment of scalable c–UAS solutions, particularly in cooperation with the U.S. Coast Guard (USCG), Customs and Border Protection (CBP), and the Department of Transportation (DOT). These agencies must be empowered and resourced to defend our maritime and other infrastructure effectively.

THE NEED FOR EXPANDED C–UAS AUTHORITIES AND THOUGHTFUL REGULATION

Today, the Federal Government's ability to detect and mitigate rogue drones remains limited to a small number of agencies under narrow statutory authorities. This patchwork is unsustainable in the face of a growing and evolving threat.

I had the privilege of co-chairing the FAA's Section 383 UAS Detection and Mitigation Systems Aviation Rulemaking Committee, which brought together industry, Government, and civil society to assess the legal and operational challenges of c–UAS deployments. One resounding conclusion: More entities need clearly-defined, narrowly-tailored authorities to engage in drone detection and mitigation activities, especially those protecting high-risk infrastructure.

We urge Congress to act on the committee's recommendations, create a legal framework for authorized detection and mitigation operations, and ensure interagency coordination, privacy protections, and operator transparency.[9]

Congress should pass the bipartisan Disabling Enemy Flight Entry and Neutralizing Suspect Equipment (DEFENSE) Act which aims to protect outdoor sporting events from unauthorized drones and enhances security at major outdoor gatherings and sporting events by ensuring that State and local law enforcement have the authority and tools necessary to protect these events from aerial threats in real time, rather than waiting for Federal intervention. The bill would give State and local law enforcement the authority to mitigate threats posed by drones in places where a temporary flight restriction is in place. This includes large outdoor and sporting events. It would also require DOJ, FAA, FCC, and the National Telecommunications and Information Administration (NTIA) to create a list of approved technology that local and State law enforcement officers can use to address these threats.

Additionally, it is imperative that Congress consider broad c–UAS legislation this Congress. Whether it is a refreshed version of the Counter-UAS Authority Security,

---

[7] *AUVSI—Rethinking Acquisition to Unleash American Leadership in Uncrewed Systems.*

[8] *AUVSI Testifies at Congressional Hearing on the State of America's Maritime Infrastructure.*

[9] *UAS Detection and Mitigation Systems Aviation Rulemaking Committee Final Report.* January 9, 2024.

Safety, and Reauthorization Act from the 118th Congress,[10] which this committee worked diligently on, or a something akin to the Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act,[11] our country and threat landscape needs 3 critical things—modernization, protection, and progress.

CONCLUSION AND RECOMMENDATIONS

Drone technology is transforming the landscape of transportation and maritime security, creating both unprecedented capabilities and new avenues of risk. As we've seen on the global stage, drones can be tools of war, espionage, and disruption. But they are also indispensable assets in defending the homeland, securing our infrastructure, and responding to emergencies with speed and precision.

As the threats are evolving rapidly, so must our policies, capabilities, and posture. The time for Federal leadership is now.

To meet this call to action, AUVSI recommends that Congress take the following actions:

1. Expand c–UAS authorities to additional Federal agencies and delegate detection authorities to State, local, Tribal, and territorial (SLTT) agencies operating at critical sites, with appropriate and robust Federal training and oversight, and delegate mitigation authorities in more limited instances, again with significant Federal training and oversight.
2. Enact legislation restricting PRC-manufactured drones from use in critical infrastructure environments, inclusive of a suitable transition period, and a funding stream that provides support for operators to transition their fleets away from unsecure PRC platforms to secure domestic or allied alternatives.[12]
3. Support domestic drone production and adoption of secure, trusted systems through advanced market commitments, grant programs, tax incentives, loan guarantees, and other Federal mechanisms.
4. Invest in detection, Remote ID, and mitigation technologies, including maritime applications.
5. Promote interagency coordination through unified national strategies and continued stakeholder engagement.

Thank you again for the opportunity to testify today, as well as the committee's leadership and focus on these urgent issues. AUVSI and its members stand ready to support this committee and the broader Congress in advancing smart, secure, and future-ready drone policies that defend our homeland while enabling innovation and trusted use.

I look forward to your questions.

Mr. GIMENEZ. Thank you, Mr. Robbins.

Members will be recognized by order of seniority for their 5 minutes of questioning. I now recognize myself for 5 minutes of questioning.

A lot of the testimony I think hits the point that we can either be reactive when it happens or we can actually be proactive now and start to address this issue.

Some 25 years ago, some manned aircraft systems were used to perpetrate the largest terrorist attack in American history.

My fear is that in the not-too-distant future unmanned systems will perpetrate the largest terrorist attack in American history using drones, obviously.

This is not something that's new to me. In 2017, I traveled to Israel when I was mayor of Miami-Dade County. We operate Miami International Airport. I went there with the explicit purpose of finding out from the Israelis what they did to protect their airports from drones, AI drones. I know we can protect ourselves from piloted drones, but AI drones.

Their solution at the time was eagles. I just don't think we just have enough eagles to go around to do that.

---

[10] *https://www.Congress.gov/bill/118th-congress/house-bill/8610/text/*.
[11] *https://www.Congress.gov/bill/118th-congress/house-bill/4333/text/*.
[12] *Whitepaper: AUVSI Partnership for Drone Competitiveness.*

So we haven't done much since then. Drone technology has just gotten worse—I mean, gotten more and more advanced—and I think the threat is expanding.

We talk a lot about authorities, and so let me put an assumption to you.

If a drone, an AI drone, were to interfere or incur into an airport, say, the airport space, would that airport have the authority to deal with it in a kinetic fashion, in a way to knock it down in whatever way?

If you can't do it through signal interruption, is there any way that that airport, does it have the authority to bring it down, even though they may know it poses an unbelievable risk to their passengers?

Mr. ROBBINS. No, sir.

Mr. GIMENEZ. We do not have that authority?

Mr. ROBBINS. No, sir.

Mr. GIMENEZ. OK.

Does anybody have that authority?

Mr. ROBBINS. In a very limited fashion, the Department of Defense, the Department of Justice, the Department of Homeland Security, and the Department of Energy have the authority to mitigate a rogue drone.

It's not a standing authority. They can't just be doing that all of the time. The way Congress has restricted the authority at the moment, it has to go through a very specific approval process and requires a very high-level signature, usually at like the deputy secretary level or higher.

Mr. GIMENEZ. Let me put an example to you. What happened in Ukraine, what the Ukrainians did to the Russians, it should be a wake-up call to us and a call to action, because had that happened here in the United States, let's say a coordinated attack on major airports, yes, there would be loss of life, there would be injury, there would be a lot of damage.

But there's something else that we're not thinking about. It's the economic damage that it does. In Miami-Dade County alone, Miami International Airport is the single largest economic generator of that county, 40,000 people directly employed by that airport, 300,000 people indirectly employed by that airport.

If you had that kind of attack in the United States and, say, across the world, you could ground air transportation to a halt—to a halt—and that would cause irreparable economic damage.

So I'm committed and hopefully my colleagues on the other side of the aisle should be committed to confronting this head-on. We need to do this now. Because, like you said, also I live in Miami and we have things called hurricanes. Hurricanes aren't a question of if. It's a question of when. I consider this threat by drones not to be a question of if. It's a question of when.

The question is, then, are we going to be proactive against it and try to mitigate that or are we going to say, "Oh my God," and then do all kinds of stuff after the fact.

So what kind of legislation do we need in order to break through the barriers and actually give our State, local, and Federal agencies the power that they need, the authorities that they need in order to protect the American public?

Who would be best to answer that?

Mr. Walker.

Mr. WALKER. Thank you, Chairman.

I think I would challenge the presumption that the immediate need is to be able to develop a reactionary device or a reactionary element to the strategy. I think a more important component is that right now we don't have awareness of the air space.

So we don't necessarily know whether the drone that's in—recently, as you know, in Miami a drone was spotted at 4,000 feet above the Miami airport.

The question was: What was that drone? Who was flying that drone? What was their mission?

So we can't automatically make the assumption that just because a drone is operating within 3 miles or 5 miles of an airport that it is necessarily hostile. So we need to start with understanding what is in the air space.

Right now we have no integrated air space management solution that tells us who's operating, what platform they're operating, and what are their intents. Therefore, we also have no way to be able to authorize those flights and deauthorize those flights to be able to separate potentially hostile from nonhostile or friend from foe.

So we have to start with: How do we identify what's in the air space? Is it a threat? Then from that point determine what we're going to authorize legislatively as the appropriate response to those threats. I think we have to start there first.

Mr. GIMENEZ. I will disagree on one point. I think we have to do all of the above at the same time. We have to find out what's out there, but also if it becomes—if we know it's hostile, we need to take action against it.

So my time is up, and I recognize the Ranking Member.

Mrs. MCIVER. Thank you so much.

Thank you all for your testimonies today.

Mr. Robbins, am I saying that right? Robbins?

Mr. ROBBINS. Yes, ma'am.

Mrs. MCIVER. OK. Robbins. I want to make sure I get it right.

Mr. ROBBINS. Thank you, ma'am.

Mrs. MCIVER. Thank you for joining us today again.

As you are well aware, expanding counter-drone authorities to additional government agencies and potentially State and local law enforcement is a complicated task. Agencies must ensure careful coordination to avoid unintended consequences that counter-drone systems can have on air space safety, especially in urban environments and near airports.

In March, the Secret Service allegedly operated a counter-drone system without appropriate coordination with interagency partners, including the FAA. The system reportedly operated outside of the approved frequencies, resulting in automated alerts to the pilots of several aircraft flying around DCA airport, which could have had an adverse impact to flight safety.

With that being said, what can be learned from this incident?

Mr. ROBBINS. Great question, ma'am. Thank you so much.

First and foremost, I think it's important that there is a hot wash from that incident and that the lessons are understood and distributed to all currently Federally-authorized users to learn les-

sons from what occurred in that incident so it doesn't happen again elsewhere in the Nation.

But I think one of the elements that we can also take is training and delegating authority to State, local, Tribal, territorial law enforcement is not entirely new to the Federal Government.

There are programs that exist now that include explosive ordnance disposal and SWAT team training that are typically held at the Federal level and then delegated down to the State level through training programs, as well as with Federal grants as well.

There's training facilities at Quantico, in Huntsville, Alabama, and other places around the country where State and local law enforcement go and they learn from our Nation's very best operators, and then they are deputized to go out and do these kind of more difficult missions.

Not necessarily every public safety official, therefore, should be a counter-UAS operator, but some should be and go through very rigorous training.

Then it is incumbent upon Congress, in my view, to then provide oversight of that program and how is it going. In the same way that you're providing oversight on the Secret Service incident, providing oversight on the future authorities that are delegated down.

Thank you, ma'am.

Mrs. MCIVER. Thank you so much for that. That was my Part 2 question about what can Congress do. But thank you so much for that, because I am always preaching about oversight, which is extremely important.

Mr. Feddersen, I understand you have experience working within the Executive branch, including at the National Security Council. What can we as legislators do to help ensure appropriate interagency coordination within the Executive branch?

Mr. FEDDERSEN. I think the actual interagency coordination is on-going and moving well. Obviously, there was a missed connection with the last incident that you mentioned.

However, I'd like it to be known that out of the 5-year pilot program for Federal law enforcement, now 7 years into the program, that was the first and only publicly-broadcast issue that they've had.

I know there is a concern with, again, moving that to private security or moving it to State and local law enforcement, but out of 7 years, 1 incident, and it was deconflicted following the incident.

They have interagency processes in place to go ahead and deal with an investigation, to follow up and correct those issues.

So beyond that, I think it's just transparency between—I know some departments and agencies are a little slow to respond to Congressional requests for reports, but I think that is, again, just transparency, communication, and coordination.

I know that the interagency is talking about this issue. I know the interagency wishes that we'd have the expansion authorities. DHS, DOJ, and the FAA have all commented on expansion authorities.

I think, to wrap up that question, I think it's important to understand that there is no reason today why detection authorities and mitigation authorities cannot be expanded so long as the individuals are properly trained.

Mrs. MCIVER. Thank you. Thank you so much for that.

I'm short on time for my next question about drones flying over New Jersey. For some reason, they seem to love New Jersey.

But with that, I'll yield back, Chairman. Thank you.

Mr. GIMENEZ. Thank you, Ranking Member.

I'll recognize the gentleman from Arizona, Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman.

Thank you guys for showing up today.

Obviously, this is a very serious topic. I don't think that most Americans have the slightest idea how warfare is evolving, especially over in the Middle East and Europe right now when it comes to drones, and that greatly concerns me as somebody who sits on the Homeland Security Committee.

A couple weeks ago up here in the District of Columbia we were down in the SCIF getting a secret briefing from several of the agencies on our drone capabilities pertaining to many of these major events that are coming up in the United States, like the World Cup, the Olympics, et cetera.

One of the recommendations that I made was that we do everything in our power to make sure that these events take place in domes, with roofs over the top, for obvious reasons. I think that would cut down a lot and seriously mitigate attacks from drones and the effectiveness that they could have in either dropping chemicals, dropping explosives, et cetera.

One of the gentlemen in there said he would put that in his report, but he said he couldn't guarantee that it wouldn't be stripped out of the report.

I did some research and there are 10 NFL stadiums within the United States that have domes. I'll read those for you now. We got the State Farm Stadium in Arizona; Mercedes-Benz Stadium in Atlanta; AT&T Stadium, Dallas Cowboys; Ford Field, Detroit Lions; NRG Stadium, Houston, Texas; Lucas Oil Stadium, Indianapolis Colts; Allegiant Stadium, Las Vegas Raiders; SoFi Stadium, Los Angeles; U.S. Bank Stadium, Minnesota Vikings; Caesars Superdome in New Orleans.

Have any of you guys made any recommendations to the interagency or any of the other groups that are responsible for hosting these events about making sure that they do everything in their power to hold these events in domes?

Go ahead, Mr. Hutton.

Mr. HUTTON. Thank you, Congressman.

I would be happy to follow up in a Classified session to talk about some of the things that my company and others have done to support Federal law enforcement agencies at high-profile events. We have not made that specific recommendation, though it makes a lot of sense.

Mr. CRANE. Why not?

Mr. HUTTON. That's been outside of our remit. It makes a lot of sense. It's entirely possible that at the action officer tactical level that that recommendation has been made, but as a company we have not. It has not come across our path. However——

Mr. CRANE. Thank you for that.

Let me ask you a follow-up, Mr. Hutton. I know you can't give me a specific here. But what percentage do you think that that

would cut down the threat if we were to host the Olympics and these World Cup games in domes when it comes to drone warfare?

Mr. HUTTON. I think that would take a significant risk off the table.

Mr. CRANE. OK. Would you commit to pass that along and help me amplify that message to FIFA and everybody involved in homeland security and protecting Americans?

Because I also looked up the average stadium size for the World Cup coming up, and it's between 64,000 to 105,000 Americans.

If we don't think for a second that terrorists and other State actors who would be willing to commit an attack on U.S. soil doesn't see that as a fat, juicy, vulnerable target, we're out of our minds.

Would you commit to helping me amplify that, Mr. Hutton?

Mr. HUTTON. I'd be happy to.

Mr. CRANE. What about the rest of you guys?

Mr. ROBBINS. Yes, sir.

Mr. FEDDERSEN. Yes.

Mr. CRANE. OK.

Thank you. I yield back.

Mr. GIMENEZ. The gentleman yields back.

I now recognize the gentleman from New York, Mr. Kennedy.

Mr. KENNEDY. Thank you, Chairman. I want to thank you and Ranking Member McIver for holding this important hearing today.

Up in New York, we have had many conversations about the impact on drones, both positive for the communities across our State as well as the potential threats that are coming with the drones, in many ways incursions into air space. We know last year the worry, the concern, and the fright that it caused up in the Northeast, whether it be New York, New Jersey.

I'd like to know, especially being along the Canadian border, my district, the 26 New York, Buffalo Niagara region, I have 4 bridges into Canada in my district. We are also aware that many of these foreign nationalists have used drones—when I say negative—to smuggle narcotics across the border. It is part of their network.

How do we balance as a Government the positive influence of drones in our lives and the technology that society can benefit from to the real negatives that oversaturation of drones is bringing into our society?

Mr. WALKER. I appreciate that question, and I think it goes back to what we were discussing earlier. I appreciate the Congressman's question about potentially moving everybody indoors for safety and protecting against that capability.

But one of the things that you pointed out is very—is probably the most critical point here, and that is we have both good and bad actors in the air. Right now we can't identify which is which.

Whether they're flying over a bridge for appropriate purposes, not flying, flying across the border for appropriate purposes, not flying, we have to start there. We have to start by having an awareness and seeing our air space.

The NFL, for example, has reported a 4,000-percent increase. I know you pointed out that there's 10 stadiums. Ironically enough, there's 22 others and they have mostly better teams, which I don't know if that has anything to do with being indoors or outdoors.

So we have to be able to identify what's operating in that air space, be able to control and protect and restrict those operators from flying in those areas that we don't want, and then and only then should we be able to effectively initiate whether it's electronic or kinetic countermeasures.

I think that's where we have to start, and I think that fixes the problem. It also establishes public trust.

Back to the Ranking Member's question about what happened in New Jersey. The bigger issue there, I think we all know, it turns out what was there was, if were it drones, was authorized, but we didn't know that at the time and we probably should have known that at the time.

So I want to just continue to reemphasize that we need to understand what's happening, we need an integrated air space management, we need to be able to be comfortable, you as regulators, policy makers, our Americans as the general public, and first responders and law enforcement.

Mr. KENNEDY. Thank you, Mr. Walker.

Thank you all for being here and your testimony.

But, Mr. Walker, thank you for taking that question head-on.

As a leader in the industry, what are your thoughts on it? How does the industry suggest that we regulate your own industry to make it safer and to prevent these bad actors from doing harm to our communities?

Mr. WALKER. Well, the industry is working I think aggressively to both grow the industry and create systems, technologies, and our own individual policies at the operator level that protect the general public.

But we're operating in silos. We're fragmented and we're awaiting a set of standards that we can mutually agree upon that both grant policies for how we operate and then regulatory authorities for how we leverage the systems that we've created.

I think it's important—and I think Mr. Robbins said it earlier, I think everybody up here that's witnessing now—the technologies exist. This is not a technology problem. We keep talking about it as though, how do we solve this problem?

We solve this problem by getting a Congressional mandate, getting funding, and allow for innovative development programs to start testing these solutions. They've been around.

So how do we do it? The industry is ready to come together. I know we are. I know everyone else in our industry is. We just need direction, we need authority, and we need funding.

Mr. FEDDERSEN. If I can add to that, sir.

The issue is, like we said, is the technology is there and there is safe technology. The FAA has been testing and evaluating counter-UAS technology since 2019. Every one of our vendors, every one of the industry members have to go through several levels of test and evaluation at every agency, every department, and every component. It's a burden on the industry to have to do that because the Government can't share that information.

But, regardless, there are safe technologies out there that can detect, track, identify, and monitor air space and give us air domain awareness, and it can be layered.

Mr. KENNEDY. Thank you. I yield back.

Mr. GIMENEZ. The gentleman yields.

I now recognize the gentleman from Louisiana, Mr. Carter.

Mr. CARTER. Thank you, Mr. Chairman.

Thank you all for being here today.

In today's world, technology is rapidly advancing, and with that progress comes new challenges for us in Congress, the Federal agencies, and first responders at home.

Unmanned aircraft systems have become more prevalent in our daily lives. We must ensure that the safety and security of Americans are protected.

This is particularly true for my district, which covers the greater New Orleans area, home to the Superdome. I thank Mr. Crane for highlighting that we're a great place to have events. Safe, secure. We recently hosted the Super Bowl without incident, I might add. We have Final Four, Sugar Bowls, countless conventions and festivals.

As I look forward and continue to work on this committee on bipartisan legislation that empowers Federal agencies and local governments to counter the threats drones pose, and as my dear friend Mr. Kennedy just said, we know that there are great applications, we also know that there are nefarious applications. So we must continue to work to endeavor to amplify those positive ones and discourage the negative ones.

Mr. Robbins, my district and the Gulf Coast will soon be in the most active period of hurricane season. How do unauthorized and unidentified drones interfere with disaster response activities, such as search-and-rescue missions, using helicopters and drones, and what are the potential consequences for survivor recovery and response safety given the new application?

Mr. ROBBINS. Thank you for that question, Mr. Carter, and it's a serious problem. Ranking Member McIver mentioned it in her opening statement as well, as did Mr. Walker.

The incident that occurred just a couple weeks ago down in Texas in a similar situation during search-and-rescue disaster response, an unauthorized rogue drone collided with a helicopter. We had a similar incident in California last year when a scooper airplane was doing water distribution on a forest fire also was struck by a drone.

When that happens, it hurts public trust, it endangers lives, and it damages the reputation of responsible drone users across the country. We have to do better.

When there is an incident response, like a hurricane or a wildfire or a flood, there is a temporary flight restriction put in place. There is technology available that should be able to restrict the flight from occurring if the operator is responsible and looking at technology that the FAA makes available to individuals who are operating these flights.

I also think it's important to distinguish between responsible commercial operators and those that are flying commercial off-the-shelf drones that maybe they bought on Walmart or——

Mr. CARTER. Are these Walmart-type commercial drones that are purchased capable of being retrofit to do harm?

Mr. ROBBINS. They absolutely are, sir. The No. 1 seller of those drones in this country is a Chinese company called DJI, which used

to restrict their drones from flying in spaces like where there was a TFR in place or over an airport.

Last December DJI removed the geofencing on their drones, giving the operators—these are not typically commercial operators. Sometimes they are, but oftentimes they're just random people who buy a drone and sometimes do stupid things with them. They've removed the geofencing, so now they can go into a zone, like the helicopter incident in Texas, that used to not be able until DJI changed their own rules.

Mr. CARTER. How can UAS intervention mitigate the dangers of drones, particularly with the Port of New Orleans or major sporting events, as I mentioned? We know these drones at large-scale public events, free parties, Mardis Gras. I mean, I'm deathly afraid of what could happen. How do we detect and mitigate the dangers of that?

Mr. ROBBINS. Yes. As mentioned, it is not a technology problem anymore. All 3 of these companies as well as many other AUVSI member companies have technologies that provide a very complex, intimate portrait of the air space to be able to distinguish between authorized drones and unauthorized rogue drones, and then as necessary be able to take action, whether it's a kinetic or nonkinetic action, against a drone to remove it from the unauthorized air space.

Mr. CARTER. Real quickly, because I have about 29 seconds. What can local and State government do to augment what we're doing at the Federal level and what you're doing? We have local players, our State police, our State sheriffs—local sheriffs——

Mr. ROBBINS. Presently not much. You can maybe find the operator and ask him politely land the drone. But until Congress extends and expands detection and mitigation authorities and allows for delegation to State and local law enforcement, unfortunately, those individuals, those great public servants are left without many tools right now, and that's unfair to them and it's unsafe to Americans.

Mr. CARTER. My time is expired, but I'd love to dig deeper into this, Mr. Chairman. Thank you. Another time.

Thank you all.

Mr. GIMENEZ. The gentleman yields.

I now recognize the gentleman from New York, Mr. Garbarino.

Mr. GARBARINO. Thank you, Chairman. Perfect timing. Thanks for holding this great hearing today.

As the Chair of the Subcommittee on Cybersecurity and Infrastructure Protection, I'm especially concerned about the potential for foreign-manufactured drones to be exploited by adversaries to carry out cyber and physical attacks against critical systems.

Many U.S. law enforcement and municipal agencies continue to use DJI drones despite security warnings from the Department of Homeland Security and CISA.

Mr. Walker and Mr. Feddersen, from your perspectives, what are the cyber risks posed by these platforms? Do you believe agencies understand the surveillance or data exfiltration vulnerabilities they may be exposing themselves to?

Mr. Feddersen, if you want.

Mr. FEDDERSEN. Yes. So I appreciate the question, sir.

The cyber effect obviously we've seen in different formats and different forms capable of carrying a virus and injecting it into the internet of things and different places. We've seen this happen. We know it's happened several times. Anything that can connect to WiFi, Bluetooth, or anything, that connect even on the LTE bands, can inject some type of virus or some type of cybersecurity vulnerability into the system.

This is something that I know the interagency is aware of. They're trying to address it. But when it comes from all the different threat vectors out there, a cyber attack from a drone tends to fall low on the list.

It's not that it shouldn't be up on the list or it shouldn't be considered, it's just a priority-based aspect of things. But we know the potential's there. We know it's been used in the past.

Mr. GARBARINO. Mr. Walker.

Mr. WALKER. Thank you.

It's a really good question, and it's a very important matter. Essentially any time that we have interconnected devices, internet of things, on a broad scale like this, you have cybersecurity concerns.

One of the things that we proposed in our written statement was that we need to have a digital flight-authorization service that has cryptographic credentials for both the operators for the platform and for their intention, and that only when those 3 elements are fused together in an appropriate manner will we authorize that flight.

That is just one approach that we believe is appropriate to ensuring that we are strengthening our cybersecurity wall against potential vulnerabilities.

Mr. GARBARINO. Mr. Feddersen, in your answer you said that the interagencies are aware, you believe they're aware, and they're trying to address it. Wouldn't addressing it just be stop using the drones? Or, I mean, is there another way to address it?

Mr. FEDDERSEN. Honestly, the simplest way to do it is to use detection and mitigation capabilities that are out there today. I mean, the technologies and vendors that are out there can identify and stop a drone from moving into an area that may be sensitive or unprotected.

Again, when you talked about critical infrastructure, though, I think it's important for us to remember that critical infrastructure is protected by private security, not law enforcement.

So when we talk about data centers, we talk about the stadiums or anything else, or even power plants, even our nuclear plants are private security, not State and local law enforcement.

So the authorities that we talk about must be expanded to them as well if we're going to actually take care of our critical infrastructure.

Mr. GARBARINO. I've had this discussion with the NFL and a whole bunch of other people, saying these authorities need to be expanded to local law enforcement when these issues arise.

Mr. Walker, did you want to add something else? You looked like you were about to.

Any others? Do you want to add anything? OK.

Mr. Feddersen, as we've seen, our adversaries have utilized unmanned aircraft system capabilities at various activities and conflicts around the world.

Based on your work in intelligence and cyber operations, how realistic is the threat of adversaries using unmanned aircraft systems or platforms to preconflict-shaping activities, such as mapping soft targets or collecting signal intelligence inside the United States?

Mr. FEDDERSEN. It's already being used, sir. I mean, you just take a look at the borders. You take a look at the cartels. You talk to the cells that we know are inside the country. We know the agencies are actively pursuing them and going after them. But the threat is here today.

Mr. GARBARINO. It's just not the border. But what else are they mapping out that we might not have—the public doesn't know about yet or it's not on the top of their radar?

Mr. FEDDERSEN. It's pattern of life. So they watch agents. They watch officials, Government officials going to and from their house. They figure out patterns of that. They can do surveillance and figure out patterns at airports, other critical infrastructure aspects of things.

We know—and particularly prisons are being infiltrated every day with drones that are going back and forth. So, again, it's being able to figure out guard shifts, patterns, different things like that.

Mr. WALKER. Yes. I would like to add to that, Congressman.

I mean, there's been 3,000 drone flights, unauthorized and unidentified drone flights over power plants and power installations in the last 24 months alone.

We don't know who flew it, why they were there, what their intention was, and what data they collected. So sometimes it is difficult to answer your question on specifically what we're doing because we don't know who they are.

Mr. GARBARINO. I had another question, but I've run out of time. I yield back.

Thank you, Chairman.

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

I now recognize the gentlewoman from South Carolina, Mrs. Biggs.

Mrs. BIGGS. Thank you, Mr. Chairman.

The FAA has reported over 1 million registered unmanned aircraft systems, more commonly known as drones, as of April 2025, with many more believed to be unregistered.

Unauthorized drone incursions are increasing in frequency, particularly in proximity to sensitive sites, such as military installations, nuclear power plants, which were just mentioned, and airports.

Between 2022 and 2024, North American Aerospace Defense Command and the Department of Defense documented more than 600 unauthorized drone overflights of U.S. military facilities.

Public reporting has also noted concerning incidents near critical infrastructure, such as the appearance of low-altitude drones over nuclear facilities and near commercial airport perimeters in multiple States.

So I think all of you are perfectly capable of answering my question, so I'll just leave it open.

But my first question is, what are some of the direct impacts of unauthorized drone overflights at military facilities, airports, and maritime ports?

Specifically for airports and maritime ports, could you explain the potential cascading effects that such incidents could or may have regionally or even nationwide?

Mr. ROBBINS. I'm happy to take that question, Congresswoman, and thank you very much.

I think, first and foremost, obviously, there's with each incident the potential for there being some sort of a catastrophic event.

Thankfully, as mentioned, we haven't seen that in the United States as yet, but we have seen it overseas, as the topic of this overall hearing, of how drone warfare abroad is changing the situation at home.

But even without those catastrophic events, each time one of these incidents occurs it erodes public trust as well. It also damages the public perception around the positive utility of drones.

At AUVSI we represent companies that focus on the defense against drones. But we also represent dozens of drone operators that are doing lifesaving critical missions every day, whether it's for public safety or package delivery or other really important things for our economy and public safety. All of that could go away if there's a very terrible drone incident that occurs in the United States.

Again, as we've talked about today, this is no longer a technology problem. The technology is in place. These 3 companies, as well as others, all have the ability to offer the protection to all the different sites that you listed.

But Congress hasn't updated the rules since 2018. Obviously, the landscape and the threat environment have changed dramatically. It's incumbent upon you as lawmakers to give Federal officials more authorities and to be able to delegate those authorities with proper training and oversight to local and State police as well.

Mrs. BIGGS. Thank you so much.

Mr. FEDDERSEN. I think there's 2 things to add back on there. I think one of it is really kind-of a lexicon we've had for a while. We should get rid of careless and clueless. Just like a vehicle on the road and our highways, you either drive it legally or you drive it illegally. The enforcement aspect of that needs to be understood.

I think also when we say counter-drone or counter-UAS, I think sometimes that's a misnomer. Again, these systems provide air domain awareness. They are a safety tool. More than everything else, they provide safety to the general public, to any of the events that we have.

The security element is there in mitigation which is also necessary. It's making sure that you have the exact tools that you need to enforce what crimes are being committed and then take appropriate action through the judicial process.

Mrs. BIGGS. Thank you so much for your insight.

Mr. Walker, I have a quick question for you.

From an industry perspective, what are the most effective tools available today to detect and neutralize these threats before they cause harm? Are private operators and owners of critical infrastructure equipped to use them?

Mr. WALKER. That's a very good question.

So first you have to understand that there are a variety of technologies out there, from RF detection, acoustic, we could go down the list of the various different ways to detect these devices. Everybody's technology is—everybody's system is an amalgamation of a very specific group of technologies.

But, no, not everybody has the availability of that. I've spoken with multiple law enforcement agencies who don't even know these technologies exist, much less have access to them.

So I think back to what everybody here has been saying. First off, do we need to give—and I really appreciate him pointing out that I think there's a fear about delegating counter-UAS authority down to certain agencies because everybody just assumes that that means we're going to be shooting down drones or taking down drones and that's not necessarily the case. It is the identification of whether or not these are hostile or not hostile.

There's, again, we've said it enough, but I'm going to say it one more time, it's not a technology problem. They exist.

Do the appropriate law enforcement agencies at all various different levels have access to these technologies? They don't. They don't have access to the training for them either.

So there's a lot Congress can do to help make this situation a lot better and fast.

Mrs. BIGGS. Thank you.

I yield back.

Mr. GIMENEZ. The gentlewoman yields back.

We're going to go through a second round of questioning here, and I'll ask each of you to please answer this.

Mr. Hutton, are you worried about a catastrophic drone attack happening in the United States?

Mr. HUTTON. It's a very short space between the inconvenience that we have seen to date—shutting down airports, raising alarm bells—and a catastrophe.

Mr. GIMENEZ. Are you worried about a catastrophic drone attack on the United States?

Mr. HUTTON. It's very worrisome, yes. The answer is yes.

Mr. GIMENEZ. Mr. Walker.

Mr. WALKER. Yes, sir.

Mr. GIMENEZ. Mr. Feddersen.

Mr. FEDDERSEN. Absolutely.

Mr. GIMENEZ. Mr. Robbins.

Mr. ROBBINS. Yes, sir.

Mr. GIMENEZ. Would you consider that—I mean, you're right, that we've seen the enemy and probably the enemy is right here, that we haven't given the authorities and we have a fragmented defense system against drones.

There's 2 levels really. There's the reckless, the reckless drone operator that puts life in danger, not because they're nefarious, but because they're reckless. They're flying somewhere they shouldn't be flying. Then there's nefarious. There's different ways to deal with each one.

Will you help this subcommittee identify the different agencies or different even committees of jurisdiction that we need to bring into

focus so that we have a comprehensive policy in defense of our homeland? Would you commit to do that?

Mr. Hutton.

Mr. HUTTON. Absolutely.

Mr. GIMENEZ. Mr. Walker.

Mr. WALKER. Yes, sir.

Mr. GIMENEZ. Mr. Feddersen.

Mr. FEDDERSEN. Yes, sir.

Mr. GIMENEZ. Mr. Robbins.

Mr. FEDDERSEN. We recommend a tiger team so those jurisdictions can actually coordinate in a rapid manner.

Mr. GIMENEZ. Mr. Robbins.

Mr. ROBBINS. Absolutely, yes, sir.

Mr. GIMENEZ. Look, I put this hearing together, but I don't know every single committee that has jurisdiction on this. I'm sure the FAA, which is part of Transportation and Infrastructure, and maybe Judiciary has it. But somehow we've got a disjointed defense mechanism here, and we need to bring it together.

This committee was formed in the aftermath of 9/11 to provide for the security of the homeland. We don't have all the jurisdiction to provide for that. Absent that, we need to make sure that we coordinate that with the other committees.

So I'm afraid that—and I hope not—but I hope that we don't have to have an incident similar to 9/11 for us to come together as a Congress and say these are the things that we need to do to counter this threat, these are the things that we need to do to counter cybersecurity threats that we have that also can be quite devastating also.

So I want to thank you for volunteering. The staff of this subcommittee will get with you all. Then we'll also have some other—we'll contact other folks.

What it is that this subcommittee, this committee needs to do in order to coordinate this so that we do come up with a strategy and an adequate defense of the homeland? Because, as you can tell, I'm really scared about this, and I think it's just a matter of time.

Since we've already—9/11, you can say, "Gee, nobody thought about that." Well, we've thought about this now. If we fail in this, it's our failure. We can't just sit in a room and think about it. We are thinking about it and we need to do something about it.

I yield the rest of my time back. I now yield to the Ranking Member.

Mrs. MCIVER. Thank you so much, Mr. Chairman.

This gives me the opportunity to talk about drones flying over New Jersey.

As many of you know, last year we had the situation where there were tons of drones flying over different parts of New Jersey, which honestly sent people in a frantic. You can understand why. Even to this day, there are still drones flying over New Jersey.

My sister was driving down the Garden State Parkway the other day, and she literally freaked out because she said she saw like a drone flying so close to the parkway, and it was just very scary. Honestly, it kind-of gave people a feeling where it's like an aircraft out of space somewhere. You're like, "What is happening?" because

people are not used to seeing drones just flying over them. So it continues to be a problem in New Jersey.

We have been given information from the Government about how these drones were not dangerous, they were OK, nothing. But, honestly, I'm not even quite sure if they understood where the drones—where they belong to, who they belong to, and can say that they weren't dangerous. We just don't know.

It doesn't seem confident that there is concrete, really good information coming from the Government about these drones flying, especially when you have so many and you can't really pinpoint where they are coming from.

So we've spent the last hour-and-a-half talking with you all, all of you sharing your expertise of what we should be doing, where we should be focused at. Hopefully, we lead this committee to really put some meat to the bone on this matter.

When we come out of it, I think one of the things that one of you said was about the oversight, having oversight. But I just think we need a more in-depth situation and process of how we are countering, especially these drones that we just cannot determine where they are coming from.

So I would love to learn more or learn more from you, for you to discuss—and anyone—honestly, I would love to hear from each of you of what we've learned from these incidents in terms of the Government's domain awareness and the public's understanding, shall I say, with drone rules and regulations, because that's a problem too.

Many people, if you see this thing flying over your backyard, people just don't even understand what is happening, what is the process, what is the procedure that these drones should just be flying? Who should they call? Like who should I call if I see this drone? First, they're getting on Facebook, first of all, like tagging me and everyone else that they can think of about what is happening.

But what is your input on that?

Mr. FEDDERSEN. I appreciate the question.

I'd like to start with the idea that these processes are already in place. Again, if anybody has issues in the community, they call their local law enforcement. If there's a security issue at a private site, security knows who to kind-of call and kind-of run into it.

So, again, if State and local law enforcement or private security would have had the technology in place at that point and the authority to detect and the authority to mitigate, they can identify drones and are able to call the FAA and find out whether or not they're authorized or not authorized.

There is equipment, including ours, where you can whitelist drones so you know whether a drone is actually authorized to fly in a certain area or not authorized to fly in a certain area. You can deconflict and focus your security efforts that way.

But it has to be decentralized, it has to be pushed to the lowest level in order for the process to work.

Mrs. MCIVER. Thank you so much for that.

Mr. WALKER. Here is what you didn't know, and this is part of the problem. Right now we have no integrated system which ties the operator and their qualifications and their certifications to operate digitally to the platform that they are operating and to their

intent where you can immediately identify who that is operating. That's the point that we've been trying to make for a long time, is, yes, it's great that we can go out and we see that drone.

But to your point, you should have had no concern as a Member of Congress or as a member of the general public that that drone is operating appropriately and is authorized. There should not be that fear.

If you go back to what happened earlier in New Jersey, the answer was nobody knew because there was no system that provided the regulators and the air space policy managers a way to determine whether those flights were appropriate or inappropriate. We have to start there.

Mrs. MCIVER. Thank you so much for that, Mr. Walker.

Mr. Robinson.

Mr. ROBBINS. Yes, I'd just add to that.

I think it also speaks to that erosion of public trust around drones. The drones that are still flying in New Jersey are more than likely doing some sort of important mission—infrastructure inspection, public safety, package delivery, things of that nature.

Compare the erosion of public trust in New Jersey, though, to north Texas, where drone operations have been authorized in a trial program by the FAA to do significant operations in the north Texas area.

People are—like communities are fighting over who gets drone delivery next, whose public safety agency is going to get the drone operations to help extend the operational reach of their local police.

So the inverse of that is when drones are authorized and the community becomes familiar with them, they become a huge asset to the community and a boost to public safety.

Mrs. MCIVER. Thank you so much for that.

Mr. Robbins. I wanted to call you Mr. Robinson. Again, I'm sorry.

Mr. ROBBINS. It's OK, ma'am.

Mrs. MCIVER. I'm out of time. So forgive me, Mr. Hutton.

Thank you.

Mr. GIMENEZ. Thank you. The Ranking Member yields back.

I now recognize the gentleman from Texas, Mr. Pfluger.

Mr. PFLUGER. Thank you, Mr. Chairman. Thanks for holding this. This is a continuation of multiple hearings that we've had, and I have been personally concerned about this for a number of reasons.

But I'll start with just a statement about the fact that the weekend's and last week's tragedies that happened in Texas, which we were involved in, had several local and State law enforcement officials reach out and say, "What are we going to do?" Because the Chinese-made technology is allowing them to do things like search and rescue. But, obviously, we're concerned about that, and we have stated those concerns in this hearing and for at least 2, maybe 3 or 4 years.

So not really a question so much as a statement of, like, how do we go faster? How do we get to a point where we can keep up with that technology?

Then I'll go to Mr. Hutton on the conversation of Ukraine, which I've spent a lot of time studying.

The iterative nature of the drones that we are seeing in that conflict is quite alarming. I'm not sure that we're keeping up. So it's kind-of in the same vein as what I've mentioned about some of our law enforcement needs.

But what features of these drones raise concern of similar tactics, techniques, and procedures being used here against us, whether it be critical infrastructure, military bases, or the like?

Mr. HUTTON. You put your finger on it, Congressman. Not just the technology, but also the tactics, techniques, and procedures are iterating at an incredibly fast pace.

As has been mentioned already, prior to your arrival, the Operation Spiderweb in Ukraine demonstrated the control of small UAS with kinetic payloads at 2,000 miles distance, indicating that you wouldn't even have to be in the United States or even on this side of the planet to be able to conduct or execute a terrorist attack against U.S. critical infrastructure. We're there.

Mr. PFLUGER. So with that statement, Mr. Feddersen, let's think about the truck, the 18-wheeler truck that the Ukrainians deployed against the Russian airplanes and fighter aircraft.

Is that a possibility here? Do we have a possibility of shipping containers being in our ports that have already those types of drones that are ready to go preprogrammed?

Mr. FEDDERSEN. We do. It's a scenario that's been, obviously, discussed kind-of ad nauseam in the community as to how it can happen. It can be at the ports. It can be an 18-wheeler. But it can also just be a flatbed pickup truck or any other truck that's driving around.

Mr. PFLUGER. What resources do we need that we do not have right now to both protect against some sort of critical infrastructure, military or even civilian-type attack? What do we need to think about legislatively? I will open that up. We can just go down the line. We have a minute and 40 seconds.

Mr. HUTTON. I'll move quickly.

You need a common integrated air picture. Three companies before you all make competitive products in this space. There is a supply of this capability.

Mr. PFLUGER. Who would run that air picture?

Mr. HUTTON. Well, that would depend. Probably it would have to be delegated down to the operational users using a set of standards and certifications and valuations provided for by the Federal Government.

Mr. PFLUGER. Mr. Walker.

Mr. WALKER. I think the other thing that you need to think about, sir, is the fact that it's easier to hide in a crowd. Drones in our air space right now outnumber manned aircraft 4 to 1. That's going to double by 2027. That's going to double again by 2030.

So as we're talking about the ability to defend against these threats, we have to equally be thinking about, how do we quickly identify those threats?

I know I sound like a broken record on that, but that's going to become much more concerning and much more of a challenge because we have to remember, of those drones in the air, 99 percent or better of them are performing real valuable missions that are saving and protecting American lives.

Mr. PFLUGER. Mr. Feddersen. We'll have 30 seconds. Split it with Mr. Robbins.

Mr. FEDDERSEN. Yes, real quick on the whole concept.

It's integration. So we are collaborating to compete in the space. We just need the policies to open up so that individuals can figure out what they need—there is no one silver bullet—so all the systems can talk to each other and be able to cover each other in layers.

Mr. PFLUGER. Last.

Mr. ROBBINS. As mentioned, the Congressional rules have not been updated since 2018. Expand air space awareness detection technology very broadly and expand the mitigation tools more narrowly with vigorous training and oversight of that program.

Mr. PFLUGER. We have asked, Mr. Chairman, I have asked NORAD and NORTHCOM to come and testify. I think it's imperative that they do that. Because if we're going to delegate those, and we're going to integrate with the State and local level with the common air picture, which I agree with, then they're going to play a key role, and that positive identification is absolutely key.

Thanks for holding this hearing. Yield back.

Mr. GIMENEZ. The gentleman from Texas yields.

I now recognize the gentleman from Louisiana, Mr. Carter, for a second round.

Mr. CARTER. Thank you, Mr. Chairman.

I'm going to follow up on the comments that my friend Mr. Pfluger started.

You state in your testimony that swarms of small drones are prevalent, like those that were used in Operation Spiderweb in Russia, and can be used to saturate enemy air space, overwhelm air defense systems, and execute lethal strikes.

How easy would it be for foreign governments to conduct similar attacks as Operation Spiderweb did here on U.S. soil?

Mr. ROBBINS. Well, I will say I have great confidence in our intelligence community and law enforcement that they're doing excellent work every day to keep us safe and prevent such an attack from happening in the United States.

But from a technology perspective, as mentioned, the technology is there, it could be in this country already, and——

Mr. CARTER. How easy is it for that to be conducted? Is it something that is just farfetched?

Mr. ROBBINS. No.

Mr. CARTER. Is it something, as our Chairman has just suggested, something we really—let me try to finish first—that we should not find ourself flatfooted thinking, "Oh, wow we know this has happened before"?

Chairman Gimenez has said very clearly shame on us if we fall prey to another attack. My suspicion is, as it was done there causing some $7 billion worth of damage, we are one accident away from being a victim of it ourselves.

Mr. ROBBINS. Absolutely. Completely agree with you, sir.

Mr. CARTER. I know it's been said over and over again. What can we be doing? ISIS has actively encouraged lone-wolf attacks targeting public—to target public civilian spaces. I know none of these are easy questions, and I know neither of you have easy answers

for us. But because we are on a fact-finding mission to determine how we can better empower you and others to protect our homeland, what else we can be doing?

Any of you can jump in.

Mr. Hutton, would you?

Mr. HUTTON. Three of us here in front of you provide situational awareness and mitigation technologies. Those Government agencies who would be our customers at the State and local level—and often at the Federal level—cannot buy them, they cannot—they do not have a forum to deeply learn about them and understand what capabilities are there, and if they did buy them would not have the authority to employ them.

Mr. CARTER. Given that there's so many of them in the air, you indicated, I think, Mr. Feddersen, that many of them are in fact providing useful tools. Are we able to easily identify those that have nefarious actions versus those who aren't?

The second part of the question is we know that—you mentioned DJI, which is a Chinese-owned-and-operated company that provides most of the commercial, I guess, recreational drones.

Do we know if those drones are able to capture photograph images, video, that an independent person is using perhaps just for fun? Do we know if they have access with their technology to actually use that information unbeknownst to the operator?

Mr. FEDDERSEN. Every time they update the drone. Every time it touches the internet, they get a new update to it, new profile. All that information's in there.

Going back to the question, sir, about how easy is it. It's coding and algorithms. People are doing it all the time with Raspberry Pis, creating their own 3-D printed drones, putting the control systems in there and figuring it out.

We see it with drone-like displays on a regular basis. I mean, the technology to do those swarm attacks and things are being used commercially in here.

I think one of the things that we were could all benefit from, especially after all the testing and evaluation that the U.S. Government has done on systems like ours, is to publish a list of those that have already been deemed safe to operate, safe to use, so that individuals, especially critical infrastructure, can look at a menu of options as what they want and we know that it's safe in the National Airspace System.

Mr. CARTER. Forty-six seconds. Anybody else want to weigh in on that?

Mr. Hutton.

Mr. HUTTON. Federal agencies have to have a level of certainty about the safety and reliability and effectiveness of the systems. Without the authorities to employ the systems, they don't get to the point at which they can determine whether those systems are safe, effective, and reliable.

Mr. CARTER. So the drone that looks like it's dropping off a package and the drone that looks like it's dropping off a bomb looks exactly the same, and that makes your job that much more difficult.

My time has expired.

Mr. FEDDERSEN. But that is why, again, law enforcement and trained security professionals who go through training for physical

security and threat assessment are the individuals that should have these tools in their hands today.

Mr. CARTER. Well, I would encourage, Mr. Chairman, the joint committees that are working on joint legislation, that we step up our game, because every minute that goes by that we are paralyzed by analysis we are an accident waiting to happen.

I want to be on record, along with the Chairman in this committee, in urging that the joint committees truly push forward. We cannot wait for the next accident and American lives are lost.

I yield.

Mr. GIMENEZ. I fully agree. The gentleman yields.

I now recognize the gentleman from Arizona, Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman.

A couple months back, I pulled in, asked for a meeting with several of the agencies that were in charge of protecting the Capitol for Inauguration Day. I was very concerned about the President after 2 assassination attempts.

I was also concerned about just a drone attack here, or another type of attack when you've got all the Members of Congress, all the Cabinet executives, et cetera. That's a huge, juicy target.

One of the things I learned is that Capitol Police doesn't even have the authorization to mitigate and deal with drones.

So we introduced a bill. It's H.R. 3334. I would love it if the Chairman would consider supporting this effort to give Capitol Police the ability to take down drones. I realize there is the Secret Service as well that has the capability and the authorization to do so.

But if we're not even willing to give authorization to protect the Capitol, I think that's a pretty key indicator that we're not prepared to protect the rest of the country, which I think needs to happen.

So I appreciate, Mr. Walker, you bringing up the integrated air space management needed. I know you've been beating that drum today, and I definitely appreciate it.

Back to Operation Spiderweb that we've talked about a lot today where the Ukrainians flew drones over 2,000 miles—some of the reporting says 2,800 miles—to attack Russian bombers, very sophisticated operation.

I'm glad, Mr. Hutton, you brought up the fact that some of our adversaries could launch an attack like that that mimics that attack from outside the United States. Is that correct?

Mr. HUTTON. Yes, it is.

Mr. CRANE. They could do that from a country like—or a city like Monterrey in Mexico or Ottawa or Calgary in Canada? Is that correct?

Mr. HUTTON. That's correct.

Mr. CRANE. Have you guys done any assessments on—I talked about the average stadium for the World Cup holding about 7,500 civilians. Have you guys done any analysis on what a drone swarm could do to that many citizens just watching a soccer game?

Mr. HUTTON. We know from lessons learned in Eastern Europe exactly what would happen. You could put all of them at risk, every one of them.

Mr. CRANE. Yes, absolutely. Absolutely.

Well, I appreciate you guys coming today. I want to—again, I know I've talked about this in my first round—but I want to publicly say that I think FIFA and Homeland Security should absolutely host all of these events coming up, for a short-term fix, in domes, because I think that that would greatly mitigate the threats that we're talking about today.

Because when you host it in a dome, then you start filtering people watching the games through magnetometers. There is a whole new level of threats that you have to deal with. But at least mitigate much of the drone capabilities that some of these nation-states and bad actors have as far as targeting large populations of people. We know that terrorist groups love to do that.

So I want to make sure it's stated publicly.

Mr. Carter, I think he left, but I hope that my other colleagues on the panel will consider sponsoring my bill and working with industry leaders like yourself in making sure that we're proactive and not reactive. Because as you guys know, this place moves at a snail's pace, and it almost seems as if most of the time we have to wait for a catastrophe to happen before we actually move on anything.

So thank you.

Mr. FEDDERSEN. Sir, I applaud the bill you and Mr. Perry put forward. We wholeheartedly agree the critical infrastructure here inside the NCR should be protected. We urge that we should protect the other 50 State capitals in legislation.

Mr. CRANE. Absolutely. Absolutely. Thank you.

Mr. GIMENEZ. The gentleman from Arizona yields.

I think we have really put a light on the issue and the fact that we in Congress need to focus in. We're kind-of spread out on our authorities. We need to kind-of focus this in.

You have my word that this subcommittee and the staff of the subcommittee are going to work with you to identify those areas and those other jurisdictions and other committees of jurisdictions will need to work on in order to really protect America, which is really what our job is.

As you also can see, this is a bipartisan effort. Both sides of the aisle see the threat, and both sides of the aisle are committed to try to resolve this problem before anything happens.

So I want to thank the witnesses for their valuable testimony and the Members for their questions. 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(E), the hearing record will be held open for 10 days.

Without objection, this subcommittee stands adjourned.

[Whereupon, at 11:41 a.m., the subcommittee was adjourned.]