UNMANNED AND UNCHECKED: CONFRONTING THE RISING THREAT OF MALICIOUS DRONE USE IN AMERICA

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

OF THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

TUESDAY, SEPTEMBER 16, 2025

Serial No. 119–34

Printed for the use of the Committee on the Judiciary

Available via: *http://judiciary.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

61–653 WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California
ANDY BIGGS, Arizona
TOM MCCLINTOCK, California
THOMAS P. TIFFANY, Wisconsin
THOMAS MASSIE, Kentucky
CHIP ROY, Texas
SCOTT FITZGERALD, Wisconsin
BEN CLINE, Virginia
LANCE GOODEN, Texas
JEFFERSON VAN DREW, New Jersey
TROY E. NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
HARRIET M. HAGEMAN, Wyoming
LAUREL M. LEE, Florida
WESLEY HUNT, Texas
RUSSELL FRY, South Carolina
GLENN GROTHMAN, Wisconsin
BRAD KNOTT, North Carolina
MARK HARRIS, North Carolina
ROBERT F. ONDER, JR., Missouri
DEREK SCHMIDT, Kansas
BRANDON GILL, Texas
MICHAEL BAUMGARTNER, Washington

JAMIE RASKIN, Maryland, *Ranking Member*
JERROLD NADLER, New York
ZOE LOFGREN, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
ERIC SWALWELL, California
TED LIEU, California
PRAMILA JAYAPAL, Washington
J. LUIS CORREA, California
MARY GAY SCANLON, Pennsylvania
JOE NEGUSE, Colorado
LUCY MCBATH, Georgia
DEBORAH K. ROSS, North Carolina
BECCA BALINT, Vermont
JESÚS G. "CHUY" GARCÍA, Illinois
SYDNEY KAMLAGER-DOVE, California
JARED MOSKOWITZ, Florida
DANIEL S. GOLDMAN, New York
JASMINE CROCKETT, Texas

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

ANDY BIGGS, Arizona, *Chair*

TOM TIFFANY, Wisconsin
TROY NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
LAUREL LEE, Florida
BRAD KNOTT, North Carolina

LUCY MCBATH, Georgia, *Ranking Member*
JARED MOSKOWITZ, Florida
DAN GOLDMAN, New York
STEVE COHEN, Tennessee
ERIC SWALWELL, California

CHRISTOPHER HIXON, *Majority Staff Director*
ARTHUR EWENCZYK, *Minority Staff Director*

C O N T E N T S

TUESDAY, SEPTEMBER 16, 2025

OPENING STATEMENTS

WITNESSES

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

Page

QUESTIONS AND RESPONSES FOR THE RECORD

UNMANNED AND UNCHECKED: CONFRONTING THE RISING THREAT OF MALICIOUS DRONE USE IN AMERICA

Tuesday, September 16, 2025

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

COMMITTEE ON THE JUDICIARY

Washington, DC

The Subcommittee met, pursuant to notice, at 3:09 p.m., in Room 2141, Rayburn House Office Building, the Hon. Andy Biggs [Chair of the Subcommittee] presiding.

Present: Representatives Biggs, Jordan, Tiffany, Nehls, Kiley, Knott, McBath, Raskin, and Swalwell.

Mr. BIGGS. The Subcommittee will come to order. Without objection, the Chair is authorized to declare a recess at any time. I apologize to everyone for starting a little over an hour late. We had votes that kind of took up more time than we thought. Welcome everyone to today's hearing on the rising threat of malicious drone use in America.

I now recognize the gentleman from Texas, Mr. Nehls, who will lead us in the pledge of allegiance.

Mr. NEHLS. Will you please stand and join me in honoring our Nation's flag.

ALL. I pledge allegiance to the flag of the United States of America, and to the Republic for which it stands, one Nation, under God, indivisible, with liberty and justice for all.

Mr. NEHLS. Thank you.

Mr. BIGGS. I now recognize myself for an opening statement. I appreciate everyone being here today. In this hearing we have before us, we're focusing on unmanned aerial systems and how these systems are being exploited by criminal elements. This issue is no longer confined to science fiction or battlefield environments. It is now increasingly disrupting daily life in America.

Over the past several years, UAS technology has rapidly advanced, becoming more affordable, more accessible, and more capable. While this has fueled innovation and commerce, public safety and emergency response, it has also led to opportunities for abuse by criminals and adversaries alike.

The threats we face today from drones are not theoretical, they are real, and they demand urgent attention. Between January and June of this year the FAA recorded more than 1,000 UAS incursions near U.S. airports. A nearly 13 percent increase from the same period last year, each of these incidents represents not just a violation of restricted airspace, but a potential catastrophe for passenger safety. Despite some progress like remote ID, our response architecture is fragmented. Remote ID helps with accountability, but does not integrate into real-time air traffic management or provide automatic alerts to airport security.

Additionally, most of our airports like dedicated counter-AUS systems. Legal restrictions further complicate matters, limiting who can respond in real time. The problem does not end with aviation safety. Criminal networks are adapting to AUS technology for nefarious purposes dropping contraband into prisons, smuggling drugs and weapons across the U.S.-Mexican border, surveilling law enforcement, and, in some case, experimenting with weaponization.

Correctional facilities are continuing to face surging drone drops of drugs, phones, and weapons. The stealth speed and GDS-guided precision of modern drones make it difficult for correctional officers to detect or intercept them without specialized training or technology. These drops enable organized criminal activity within prison walls, disrupt inmate discipline and threaten the safety of the staff and inmates alike.

The U.S. Northern Command leadership purported that over 1,000 drones crossed into U.S. airspace from the Mexican border each month with CBP agents noting that in Texas, along the Rio Grande Valley alone over 10,000 drone incursions and 25,000 drone sightings occurred in 2024.

Unlike conventional smuggling methods, drones offer cartels a cost-effective and low-risk means to deliver small payloads while avoiding direct encounters with U.S. law enforcement.

The CBP and DOD recently recorded 70 incursions in 11 days around Laredo, prompting the deployment of striker units to bolster surveillance. Equipped with features like night vision and the ability to operate below radar thresholds. These drones present a stealthy and persistent challenge to border security. Despite this growing threat, CBP lacks the authority to disable or intercept UAS in most circumstances, limiting its ability to respond effectively in real time.

National special security events, NSSEs, such as Presidential inaugurations, political conventions, high-profile sporting events are increasingly vulnerable to drone-based threats due to their symbolic value, dense crowds, and media visibility.

While Federal agencies like the U.S. Secret Service, the FBI and DHS are authorized to deploy counter-UAS capabilities and national special security events under the Preventing Emerging Threats Act of 2018, these efforts are intense and confined to a limited number of events each year.

The DOJ officials testified that counter-UAS protections are typically planned months in advance and require substantial coordination with the FAA to ensure legitimate airspace operations are not inadvertently affected. As a result, thousands of public events that

fall outside the NSSE designation like any UAS mitigation coverage, even as drone incidents rise nationally.

Expanding use of drones in public spaces also introduces new risks for first responders. An active shooter, protest or hazardous materials scenarios, the presence of unauthorized drones can obstruct airspace, delay medevac or surveillance operations, and even be used to track responder positions or deliver harmful payloads.

Many of these tools are restricted under Federal law and cannot be used by State or local entities without explicit authorization. Additionally, these systems must be miniaturized, cost-effective, and interoperable with existing emergency response infrastructure to be viable at scale.

The dominance of Chinese manufacturers, particularly DJI and the global drone market raises specific espionage concerns. Under Chinese law, companies are legally obligated to cooperate with Chinese national intelligence authorities, which amplifies the risk that drones supplied by these firms can transmit sensitive data back to foreign governments.

As of today, DJI holds nearly 90 percent of the consumer drone market, and approximately 75 percent in commercial sectors. Multiple policy reviews and commentaries warn that adversarial actors may exploit the supply chain vulnerabilities, together intelligence on U.S. critical infrastructure, military bases, research facilities, and emergency operations. The threat is persistent and accelerating, and it will take a coordinated alignment of resources, technology and authorities to contain it. This hearing serves an important step to confront and combat malicious drone use across the country and beyond.

I look forward to hearing what our witnesses say in our lively discussion.

Now, without objection, I want to enter into the record an article entitled, "Increasing Drone Incidents Near U.S. Airports, Stadiums Prompt Alarm Officials Say"; and "Drones Lifting Inmates Out of Prisons? U.K. Inspector Says It Is a Theoretical Possibility."

Without objection. Now, I yield back and recognize the Ranking Member of the entire Committee, Mr. Raskin, for his opening statement.

Mr. RASKIN. Thank you, Mr. Chair, for holding this hearing on the rising threat posed by an unmanned aircraft systems commonly known as drones. The FAA reports that over one million drones are now registered in the U.S. for a broad range of commercial and recreational purposes; government agencies also use them to improve diverse public safety operations, including search and rescue, disaster response, crime scene investigation, and even traffic enforcement. Like any technology, including AI-enabled technology, which this Subcommittee discussed earlier in the summer, drones can also be used for unlawful purposes, like delivering contraband to inmates in prison, or ferrying Fentanyl across the Northern and Southern borders of our country.

In 2023, in my home State in Maryland, 15 people were indicted as part of a criminal network that used drones to smuggle Fentanyl and other drugs, cell phones, tools and other contraband into the Roxbury Correctional Institution in Hagerstown. I'm sure

that many of my colleagues have similar stories from their own States.

The DOJ is one of five Federal agencies with drone detection and mitigation authority, which allows the Department to detect, track, and even destroy drones that pose a credible threat to Federal court houses, prisons, and large gatherings. The FBI and the Federal Bureau of Prisons are also able to utilize some counter-drone detection systems. In fact, earlier this year, BOP reported the agency has deployed such systems at 64 facilities which have helped detect malicious drone use, better inform law enforcement of incoming threats, and locate suspected criminal drone operators.

Today, as we discuss law enforcement efforts to respond to the malicious drone activity and the use of drones to enhance public safety, we must be mindful of the risks associated with the detection and mitigation of drones, as well as the need to respect the privacy interest and civil liberties of the public in the process. Let's make sure that law enforcement uses both drone and counter-drone technology correctly, safely, and always within the bounds of the law. That's why I was pleased to join the Chairs and Ranking Members of the Transportation Infrastructure Committee and the Homeland Security Committee to introduce H.R. 5061, The Counter-UAS Authority Security, Safety, and Reauthorization Act. The bill, which was reported favorably by the Transportation and Infrastructure Committee by remarkable vote of 60–0, would reauthorize, reform and expand the existing counter unmanned aircraft system or counter-UAS authorities of Homeland Security Department and the DOJ. Among other provisions the bipartisan bill would, for the first time, expand these authorities to State and local law enforcement through a carefully calibrated pilot program.

The bill would also establish training program for these agencies to meet before they can operate counter-UAS systems in minimum performance requirements for counter-UAS technology before it can be deployed ensuring these systems are used safely and solely within the strictures of the law.

I trust today's hearing will commit to my colleagues the need to support this bill, and then we will see swift unanimous passage of it.

Thank you, Mr. Chair. Thanks to all our witnesses to being here. I look forward to hearing from you. I yield back.

Mr. BIGGS. The gentleman yields back. Thank you.

Without objection, all other opening statements will be included in the record. Now, we will introduce today's witnesses.

We will begin with Dr. Catherine Cahill. Dr. Cahill is the Director of the Alaska Center for Unmanned Aircraft Systems Integration, ACUASI, and the Geophysical Institute at the University of Alaska Fairbanks.

ACUASI leads one of the seven FAA UAS test sites, as the FAA's Alaska BEYOND site and is a core university in the FAA's center of excellence for UAS research. Dr. Cahill has served as a member of the FAA's drone advisory committee and advanced aviation advisory committee. Thank you for being here with us today, Dr. Cahill.

Dr. Ryan Wallace is a Professor at Embry-Riddle Aeronautical University. His research focuses on UAS safety, security, human

factors and public policy. Dr. Wallace has conducted training seminars for Federal agencies on the topics of UAS safety operations, and counter-UAS techniques. He also serves as a representative on the FAA's drone safety team and served in the U.S. Air Force. Thank you for being with us, Dr. Wallace.

Mr. Brett Feddersen is the Vice President for strategy and government affairs at D-Fend Solutions, a manufacturer of counter-drone systems for the military, law enforcement, and others. He also serves as the Chair of Security Industry Association's drone security subcommittee. He previously served as the Executive Director for national security programs and incident response at the FAA, and in various roles at the Pentagon, the White House, the U.S. Army, and as a Pennsylvania State trooper. Thank you, Mr. Feddersen, for being with us today.

Next is Sergeant Robert Dooley. Sergeant Dooley has served for more than 22 years with the Florida highway patrol, where he is currently the UAS and C–UAS program coordinator. He developed and has led the FHP's UAS program since its inception.

Sergeant Dooley is an expert in law enforcement, UAS operations, disaster response operations, and special events and high value target UAS security operations. Thank you all for being with us today.

We will begin by swearing you in and ask that you would each rise and raise your right hand.

Do you swear or affirm under the penalty of perjury that the testimony you are about to give is true and correct to the best of your knowledge, information, and belief, so help you God?

The record will reflect that the witnesses have each answered in the affirmative. Thank you, please be seated.

Each of you should know that your written testimony will be entered into the record in its entirety. Accordingly, we ask that you summarize your testimony in five minutes. We're going to begin today with Sergeant Dooley, so you're recognized for your five minutes. I'll just tell you should see a clock in front of you. When you're about 10 seconds, before you hit the five, I will start tapping like this, that means please wrap it up. We'll try to be a little bit lenient because we appreciate you being here, but we would ask you to stay five minutes because we all have your testimony, we've all read your testimony.

Sergeant Dooley, you're first.

STATEMENT OF SGT. ROBERT DOOLEY

Sgt. DOOLEY. Thank you and good afternoon. Again, I'm Sergeant Robert Dooley of Florida Highway Patrol. I am our statewide coordinator for unmanned operations.

The critical importance of drone detection and mitigation for public safety as unmanned aircraft systems continue to proliferate across recreational, commercial, and malicious domains. The ability of public safety agencies to detect and mitigate unauthorized or threatening drones has become a national imperative.

This statement outlines the growing threat landscape associated with drones and discuss the current challenges, detection, and mitigation, and advocates for urgent integration of counter-UAS capabilities within a broader spectrum of public safety framework.

The rapid evolution and accessibility of drone technology have transformed industries. revolutionized emergency response, and public safety operations. However, with this growth comes an increasing threat of misuse, whether intentional or neglect, from contraband drops over prison yards to surveillance of critical infrastructure and interruptions of emergency scenes, public safety agencies now face the complex airspace risk. The ability to detect, track, identify, and when necessary, mitigate rogue drones is essential for protecting lives, preserving critical infrastructure and ensuring operational integrity.

Drones present a unique set of challenges to public safety. As you spoke earlier, criminal exploitation, criminal organizations increasingly use drones to smuggle drones to smuggle drugs, weapons, and contraband into correctional facilities or across the borders, terrorist use, adversarial State and non-State actors have experimented with drones for surveillance and weaponization, creating low-cost and low-detection threat vectors.

Privacy violations and harassment: Drones can be used to stalk, harass, or violate the privacy of civilians and law enforcement officers often in ways that are difficult to detect and prevent.

Interference with public safety operations: Unauthorized drones flying near traffic crashes, fire scenes, disaster zones can impede emergency response, creating hazardous responses for both responders and civilians.

The need for detection and mitigation capabilities: Public safety agencies must be able to detect, identify and if authorized, mitigate UAS threats in real time. Without this capability, agencies operate blindly in shared airspace, increasing risk to both responders and the public. The key benefits of these capabilities include situational awareness, drone detection systems enhance airspace awareness, allowing agencies to monitor aerial activity near sensitive locations or at the scenes.

Threat identification: Identifying type, intent and operator of drone is essential for appropriate response and legal action. Incident mitigation in critical scenario stopping or redirecting a drone may be necessary to prevent harm or disruption, especially during mass gatherings dignitary protection or major disasters.

Current limitations in legal barriers: Despite the urgent need, most State, local, Tribal, and territorial public safety agencies lack the legal authority to mitigate and often face limitations even detecting them. Only Federal agencies currently possess this broad C–UAS authority under 6 U.S.C. 124(n) leaving a gap in homeland security at the local level.

Additionally: Technology access: C–UAS systems are costly, complex and often limited to military or Federal use.

Interagency coordination: There's a lack of real-time data sharing and standard operating procedures that could hinder unified responses.

Policy gaps: Existing Federal laws, including the FAA's preemption of airspace regulation complicate the rules and responsibility of our SLTT agencies.

Legislative reform is needed, granted, limited controlled UAS authority to vet and train public safety entities under Federal oversight as proposed in several legislative efforts. Training and stand-

ardization create a standardized C–UAS training and certification programs ensuring safety, accountability, and legal compliance.

Technology deployment: Fund and deploy scalable, nonkinetic drone detection systems to local agencies, particularly those responsible for critical infrastructure at mass events.

Public and private collaboration: Encourage partnerships between technology providers, law enforcement and Federal agencies to pilot C–UAS tools under lawful frameworks and community engagement.

Educate the public on the responsible use of drones and build awareness of the risks associated with unauthorized operations. The ability to detect and mitigate rogue drones is no longer a futuristic concept, it is a present-day necessity. Public safety professionals stand on the front lines of both natural and man-made crises and lack a C–UAS capability which leaves critical vulnerability in our national preparedness.

Federal agencies play a vital role empowering State local responders with tools, training and authority to protect their communities from aerial threats is the next essential step in securing the homeland.

I thank you and I await your questions.

[The prepared statement of Sgt. Dooley follows:]

The Critical Importance of Drone Detection and Mitigation for Public Safety

US Congress Committee on the Judiciary

September 16, 2025

Sergeant Robert Dooley – Statewide UAS / C-UAS Coordinator

RobertDooley@FLHSMV.GOV

Florida Highway Patrol

Witness BIO:

Sergeant Robert Dooley has more than 23 years of service as a Florida State Trooper, and has developed and led FHP's UAS program since inception. His expertise includes law enforcement UAS operations, both manmade and natural disaster response operations, special event and high-value target UAS security, and the legal aspects of operating Drones for Good. Sergeant Dooley regularly assists other public safety agencies and partner organizations with education and developing / enhancing their UAS programs. His broad range of experience includes working with other partner agencies at the local, state, inter-state and Federal levels, as well as lawmakers, State Attorneys, media and other community stakeholders.

Sergeant Dooley also serves as the co-founder and law enforcement lead for the DRONERESPONDERS Florida Public Safety Coordination Group (FLOGRU), where he assisted public safety and government drone users throughout Florida in transitioning their UAS fleets to Florida-compliant UAS. He serves on the Board of Directors for the Florida AUVSI chapter. Sergeant Dooley is a national FAA FAASTeam representative and sits on the IACP aviation committee.

Statement for the Record:

The Critical Importance of Drone Detection and Mitigation for Public Safety

As unmanned aircraft systems (UAS) continue to proliferate across recreational, commercial, and malicious domains, the ability of public safety agencies to detect and mitigate unauthorized or threatening drones has become a national imperative. This statement outlines the growing threat landscape associated with drones, discusses the current challenges in detection and mitigation, and advocates for the urgent integration of counter-UAS (CUAS) capabilities within the broader public safety framework.

The rapid evolution and accessibility of drone technology have transformed industries and revolutionized emergency response and public safety operations. However, with this growth comes an increasing threat of misuse—whether intentional or negligent. From contraband drops over prison yards to surveillance of critical infrastructure and interruptions of emergency scenes, public safety agencies now face a complex airspace risk. The ability to detect, track, identify, and, when necessary, mitigate rogue drones is essential for protecting lives, preserving critical infrastructure, and ensuring operational integrity.

Drones present a unique set of challenges to public safety:

- Criminal Exploitation: Criminal organizations increasingly use drones to smuggle drugs, weapons, and contraband into correctional facilities or across borders.
- Terrorist Use: Adversarial state and non-state actors have experimented with drones for surveillance and weaponization, creating a low-cost, low-detection threat vector.
- Privacy Violations and Harassment: Drones can be used to stalk, harass, or violate the privacy of civilians and law enforcement officers, often in ways that are difficult to detect and prevent.
- Interference with Public Safety Operations: Unauthorized drones flying near traffic crashes, fire scenes, or disaster zones can impede emergency response, creating hazardous conditions for both responders and civilians.

The Need for Detection and Mitigation Capabilities

Public safety agencies must be able to detect, identify, and if authorized, mitigate UAS threats in real time. Without this capacity, agencies operate blindly in a shared airspace, increasing risks to both responders and the public. Key benefits of these capabilities include:

- Situational Awareness: Drone detection systems enhance airspace awareness, allowing agencies to monitor aerial activity near sensitive locations or active scenes.
- Threat Identification and Attribution: Identifying the type, intent, and operator of a drone is essential for appropriate response and legal action.
- Incident Mitigation: In critical scenarios, stopping or redirecting a drone may be necessary to prevent harm or disruption—especially during mass gatherings, dignitary protection, or major disasters.

Current Limitations and Legal Barriers

Despite the urgent need, most state, local, tribal, and territorial (SLTT) public safety agencies lack the legal authority to mitigate drones, and often face limitations in even detecting them. Only federal agencies currently possess broad CUAS authority under 6 U.S.C. §124n, leaving a gap in homeland security at the local level.

Additionally:

- Technology Access: CUAS systems are costly, complex, and often limited to military or federal use.
- Interagency Coordination: Lack of real-time data sharing and standard operating procedures hinders unified responses.
- Policy Gaps: Existing federal laws, including the FAA's preemption of airspace regulation, complicate the roles and responsibilities of SLTT agencies.

Path Forward: Recommendations for Enhancing CUAS Capabilities

1. Legislative Reform: Grant limited, controlled CUAS authority to vetted and trained public safety entities under federal oversight, as proposed in several legislative efforts.
2. Training and Standardization: Create standardized CUAS training and certification programs, ensuring safety, accountability, and legal compliance.
3. Technology Deployment: Fund and deploy scalable, non-kinetic drone detection systems to local agencies, particularly those responsible for critical infrastructure and mass events.
4. Public-Private Collaboration: Encourage partnerships between technology providers, law enforcement, and federal agencies to pilot CUAS tools under lawful frameworks.
5. Community Engagement: Educate the public on the responsible use of drones and build awareness of the risks associated with unauthorized operations.

Conclusion

The ability to detect and mitigate rogue drones is no longer a futuristic concept—it is a present-day necessity. Public safety professionals stand on the frontlines of both natural and manmade crises, and their lack of CUAS capability leaves a critical vulnerability in our

national preparedness. While federal agencies play a vital role, empowering state and local responders with the tools, training, and authority to protect their communities from aerial threats is the next essential step in securing the homeland.

The following is what will be needed for forward movement on this topic:

Research documenting the legal framework surrounding C-UAS with special emphasis on Congressional authorizations and special exemptions.

Capabilities Research focused on the types of C-UAS technology available with special emphasis on detection and mitigation capabilities.

Certifications Research focused on developing standards, training, and certification programs for the C-UAS ecosystem.

Capacity Research focused on building capacity to implement C-UAS technologies to facilitate awareness and security in the NAS.

Accountability Research focused on developing accountability surrounding a C-UAS conceptual framework to ensure oversight and adequate protection of civil liberties.

Mr. BIGGS. Thank you, Sergeant Dooley. The Chair now recognizes Mr. Feddersen for his five minutes. Mr. Feddersen, please.

STATEMENT OF BRETT FEDDERSEN

Mr. FEDDERSEN. Good afternoon, Chair Biggs, Ranking Member Raskin, and the distinguished Members of the Subcommittee. Thank you for the honor of appearing before you today.

My name is Brett Feddersen, I am the Vice President for strategy and government affairs at D-Fend Solutions, a leading counter-drone manufacturer. I also serve as the Chair of the Security Industry Association's drone security Subcommittee, a group comprised of leading providers and end users of counter drone technologies available in the world.

I commend the Subcommittee for its proactive focus on the threat and has quickly gone from a distant concern to clear and present danger to our national security, to our critical infrastructure and to our public safety. The illegal use of drones has evolved from simple nuisance and trespassing to sophisticated criminal malicious activity. The accessibility, affordability, and adaptability of this technology have given us new capabilities, most often used for good. However, they also have created significant vulnerabilities that we as a Nation are not yet prepared to face.

We can categorize these threats into three primary domains. First are criminal and illicit activities. The use of drones by criminal and terrorist organizations is no longer a hypothetical scenario. Incidents of drones being used to deliver contraband like drugs and weapons into correctional facilities are a daily occurrence across America.

The weaponization of drones has been occurring in the United States for years. The internet has brought battlefield tactics to North America, through shared lessons learned in conflicts in Europe and the Middle East. We continue to see rival cartels repeatedly conduct indiscriminate carpet-bombing attacks against other cartels using explosive laden drones.

In 2021, the Jalisco New Generation Cartel created a dedicated unit of drone operators to attack rival groups in Mexico. Today, Mexican cartels are reportedly using one-way attack drones alongside the more traditional explosive carrying quadcopters. Last year, U.S. Federal authorities detected approximately 60,000 cartel drones near the border.

The second category is physical and cyber-attacks on critical infrastructure. The potential for drone attacks in critical infrastructure is alarming. A drone with a small payload could cause widespread disruption and economic turmoil by damaging power stations, water treatment plants, communication powers, or data centers.

The U.S. critical infrastructure is often protected by trained security professionals, not law enforcement. Any assumption that State and local law enforcement could fill the private sector gap is a gross underestimation of reality of police resources.

The third category is surveillance and espionage. Drones offer a low-cost, low-risk platform for persistent surveillance. They can be equipped with sophisticated cameras and sensors to gather intelligence from a distance without the need for physical access.

Drones can bypass traditional security perimeters, making them a favorite tool for illicit trade. Domestically, drones are being used to stalk, harass, and spy on people in their own homes. This invasion of privacy goes unchecked, as police watch the drones fly away without leaving a physical footprint for them to follow.

Our current legal and technological frameworks have not kept pace with these clear and growing dangers. The authority to detect and mitigate malicious drones is fragmented across the Federal agencies, creating confusion and gaps in response.

While safe and effective counter-drone technology exists today, its use is severely restricted by current laws. To address these challenges, I respectfully offer the following recommendations to the Subcommittee for consideration. A comprehensive Federal counter-drone legislation. We need clear and cohesive framework of nationwide counter-drone operations. Year after year Congress continues to introduce counter-drone legislation but never passes it. This legislation should immediately expand the legal authorities to detect, track, and identify drone threats to all Federal agencies, States, local, Tribal, and territorial law enforcement, and trained security professionals protecting our critical infrastructure.

This legislation should also expand the existing 2018 Federal pilot program for the mitigation of drone threats to those same Federal, State, local entities, and trained security professionals.

This pilot program must be launched in a robust manner to enable the rapid scaling of capabilities ahead of the World Cup, America's 250th anniversary celebration, next year's elections, and the 2028 Olympics. If these authorities are not granted by Congress quickly, then these mass gatherings will go unprotected and require Federal resources to be diverted from the border, other critical and national infrastructure missions.

In conclusion, the threat from malicious drones uses in real and immediate and growing, we must take decisive action now.

I thank you for your time and look forward to your questions.

[The prepared statement of Mr. Feddersen follows:]

Brett Feddersen
Vice President for Strategy and Government Affairs
D-Fend Solutions AD, Inc.

BEFORE

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime and Federal Government Surveillance

HEARING ENTITLED

Unmanned and Unchecked: Confronting the Rising Threat of Malicious Drone Use in America

ON

September 16, 2025
Washington, DC

INTRODUCTION

Chairman Biggs, Ranking Member McBath, and distinguished members of the Subcommittee, thank you for the honor of appearing before you today. I commend this Subcommittee for its proactive focus on a threat that has rapidly evolved from a distant concern into a clear and present danger to our national security, critical infrastructure, and public safety.

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, a group comprised of the leading providers of C-UAS technologies available around the world, as well as the security service providers and integrators that use these products to carry out critical public safety functions. Throughout my time in law enforcement, the military, and as a federal civilian, I was dedicated to the safety and security of our great nation. Now in the private sector, the mission is no different, and I am honored to appear before the Subcommittee representing both D-Fend Solutions and the drone security industry.

I am here today to discuss the rising and multifaceted threat posed by the malicious use of unmanned aircraft systems (UAS), or drones. The accessibility, affordability, and adaptability of this technology have democratized aerial capabilities. Still, in doing so, they have also created a significant vulnerability that we, as a nation, are not yet prepared to fully address.

THE EVOLVING THREAT LANDSCAPE

The malicious and illicit use of drones has evolved beyond simple nuisance to become a realm of organized, sophisticated threats and criminal activity. We can categorize this threat into three primary domains:

1. Criminal and Illicit Activities:

The use of drones by transnational criminal organizations, terrorist organizations, including cartels, domestic gangs, and individual bad actors, is no longer hypothetical. Incidents of drones being weaponized or used to deliver contraband—from drugs and weapons to cell phones—into correctional facilities are a daily occurrence. The challenge is not only at the federal level, but at state and local correctional facilities as well, all of which are often ill-equipped to detect or counter these incursions. The ability of drones to bypass traditional security perimeters makes them a favored tool for illicit trade.

2. Physical and Cyber-Attacks on Critical Infrastructure:

The potential use of drones in attacks on critical infrastructure is alarming. A drone with a small payload could significantly damage power substations, water treatment plants, or communication towers, causing widespread disruption and economic turmoil. Unauthorized incursions over sensitive sites, such as military bases and recent drone sightings in New Jersey, highlight this threat. The emergence of AI-enabled, autonomous drones adds another layer of complexity to the detection and response ecosystem.

3. Surveillance and Espionage:

Drones offer a low-cost, low-risk platform for persistent surveillance. They can be equipped with sophisticated cameras, thermal sensors, and even Wi-Fi sniffing technology to gather intelligence from

a distance, without the need for physical access. This capability is particularly concerning when considering foreign adversaries and their state-sponsored actors. The widespread use of commercially available drones manufactured by foreign entities raises significant counterintelligence risks, as data collected by these devices could be exfiltrated back to hostile governments.

CHALLENGES IN CONFRONTING THE THREAT

Despite the clear and growing danger, our current legal and technological frameworks have not kept pace. Key challenges include:

Fragmented Authorities: The authority to detect and mitigate malicious drones is fragmented across various federal agencies, including the Department of Homeland Security, the Department of Justice, the Department of Defense, and the Department of Energy. This lack of a single, unified authority across the Federal government creates confusion and potential gaps in response, especially for state and local law enforcement and trained security professionals protecting critical infrastructure.

Technological and Legal Gaps: While safe and effective Counter-UAS (C-UAS) technology exists, such as RF-Cyber takeover systems, its use is severely restricted by the interpretation of existing laws formed well before drone technology became prominent. Law enforcement has the legal authority to pursue and stop a suspicious car operating illegally, but still lacks the legal standing or authority to use technology to do the same with a drone in a safe and timely manner.

Lack of Uniformity: The FAA has made strides in regulating drone operations, but a patchwork of state and local laws has created an inconsistent legal landscape. This makes it difficult for law enforcement to act decisively and for responsible drone operators to understand and comply with regulations. It also leaves law enforcement and the public wondering what is legally or illegally flying above their communities. I cannot overstate the immediate need for clear, expanded detection, tracking, and identification authorities enough to ensure our communities have complete air-domain awareness of drone activity across America.

RECOMMENDATIONS

To address these challenges, I respectfully offer the following recommendations for the Subcommittee's consideration:

1. Comprehensive Federal C-UAS Legislation: Congress must pass legislation that provides a clear and cohesive framework for C-UAS operations across the United States. This legislation should:

- **Expand Existing C-UAS Authorities:** Clarify and expand the legal authority for all federal agencies, state, local, tribal, and territorial law enforcement, and trained security professionals protecting our critical infrastructure to use C-UAS technologies to detect, track, and identify drone threats.
- **Expand the Existing Pilot Program**: Expand the 2018 Federal Pilot Program for mitigation of drone threats to include all federal agencies, state, local, tribal, and territorial law enforcement, and trained security professionals. The original 5-year pilot program is now in its eighth year. It needs to be expanded in a manner and scale commensurate with the rapid emergence of new technologies and the growing threat to our society from the illicit use of drones. Failure to do this creates significant risk to our ability to safely and securely host the World Cup, America's

250th anniversary celebrations, hold elections, and host the 2028 Olympics.

2. Inter-Agency Collaboration and Information Sharing: An ability for law enforcement to review the FAA's drone registry information through the existing National Crime Information Center (NCIC), like we do with vehicle registration and license plates, would better enable law enforcement to protect the public in a safe and efficient manner that is consistent with current privacy and civil liberty laws.

3. Public Awareness and Education: Like operating a car, you can either fly drones legally or illegally, and after years of FAA awareness campaigns, ignorance of the law is no longer a defense for recklessly flying in our nation's airspace. We must launch a robust public awareness campaign to educate citizens on the dangers and illegality of careless and malicious drone use. This campaign should emphasize the potential for severe legal penalties for unauthorized drone operation in restricted areas.

CONCLUSION

In conclusion, the threat from malicious drone use is real, immediate, and growing. We have seen what these platforms are capable of in conflicts abroad, and we are already seeing these same tactics being adapted for use against our communities and our country.

By taking decisive action now to modernize our laws, enhance our technological capabilities, and strengthen the partnerships between all levels of government, we can ensure that our skies and citizens on the ground remain safe and that the promise of unmanned technology is never subverted by those who seek to do us harm.

Thank you, and I look forward to your questions.

Respectfully Submitted,

BRETT J. FEDDERSEN
Vice President of Strategy and Government Affairs at D-Fend Solutions AD, INC
Chair of the Security Industry Association's Drone Security Subcommittee

Mr. BIGGS. Thank you, Mr. Feddersen.

The Chair recognizes Dr. Wallace for his five minutes. Dr. Wallace.

STATEMENT OF DR. RYAN WALLACE

Dr. WALLACE. Chair Biggs, Ranking Member Raskin, and the other distinguished Committee Members. Thank you for the opportunity to testify on the important issue of protecting our Nation from the misuse of unmanned aircraft systems, sometimes referred to as UAS, or more colloquially, as drones.

My name is Ryan Wallace, and I currently serve as a Professor at Embry-Riddle Aeronautical University. For the past 10 years, my research has focused primarily on UAS safety and security threats through the use of UAS detection equipment. This use of unmanned aircraft is not fundamentally a technology problem, but rather, a people problem. What makes this problem particularly challenging is the unique aerial capabilities that UAS provides to their operators, capabilities previously limited only to those with the resources and training to operate manned aircraft. The accessibility, affordability, and automation have now placed these capabilities within the reach of anyone with a few hundred dollars. This creates a disproportionate force multiplier for bad actors.

The destructive potential of consumer drones recently came to global attention in Ukraine during the famed operation Spiders Web where small drones were used to conduct rapid, surprising, accurate, and devastating attacks. These attacks were executed with near impunity, highlighting the critical vulnerability gap posed by UAS threats. The remote nature of these attacks left no one to arrest or hold accountable.

Today, these tactics and technology are being employed both domestically and near our borders. The FAA estimates there are currently more than 2.8 million drones in the United States, nearly double the number of drones in 2018 than when the Preventing Emerging Threats Act was signed into law.

Today, UAS outnumber manned aircraft by nearly 13–1. The agency estimates that within five years, this number will grow a further 10 percent. Presently, drones are causing three major domestic problems: (1) Creating a collision risk with aircraft operating in the National Airspace System; (2) contraband delivery into prisons and correctional institutions; and (3) incursions along our borders. The potential consequences of a midair collision with a drone erode the safety of our skies. As of the second quarter of 2025, the FAA recorded a total of 1,022 sightings, approximately 170 per month with aircrew reportedly taking evasive action in 2.8 percent of those cases.

In January of this year, a Canada Air CL–415 conducting suppression operations struck a small drone operating at low altitude within a temporary flight restricted zone near the Palisades fire. Their operations were suspended to allow that fire to expand unabated, further enhancing the destruction and risk to response personnel.

According to Michael Torphy, the FBI and Christopher Hardy of the Department of Justice, drone activity has proliferated to more than half of the Bureau of Prison Federal facilities with incidents

climbing to more than 479 in 2024, nearly 20 times the number since the agency started tracking in 2018.

Similarly, Steven Willoughby from the Department of Homeland Security highlighted the extent of the porous UAS activity along the U.S. border stating, In the last six months of 2024, more than 27,000 drones were detected within 500 meters of the Southern border.

To effectively address these challenges, I offer several observations, foremost that all drone incidents are local incidents first. Often, first responders to these incidents will be sworn officers from one of the Nation's nearly 18,000 State and local law enforcement agencies. Most of these agencies lack formal training for dealing with drone incidents. Even fewer are equipped with tools to support the detection, tracking, and identification of UAS.

Currently, no State or local law enforcement agencies are equipped and authorized to forcibly take down a UAS threat without the compliance of the operator who may be positioned miles away from the aerial vehicle.

Testimony by Michael Torphy from the FBI underscored resource limitations in providing counter-UAS protection, highlighting the agency was only able to cover .05 percent of the more than 240,000 special events eligible for counter-UAS protection. Ultimately, the widespread immediate need for counter-UAS protection should be a part of calculus used to determine future authorities.

The training is a vital element in protecting our public safety personnel to respond effectively to drone instances. Foremost, it is essential to ensure both UAS detection and mitigation efforts do not create or exacerbate hazards within the National Airspace System, respect from interference with navigation or communications infrastructure, or impede air traffic management functions.

It is also necessary to educate officers on how to effectively respond, investigate, document, and charge these incidents in a manner that leads to successful prosecutions. Moreover, such training ensures reinforcement of appropriate procedures designed to protect the rights, expression, privacy, and other civil liberties. There are no magic bullet technological solutions to this problem. Each type of technology has its own inherent capabilities and limitations.

Finally, I would like to highlight the vital importance of continued research and development. Research consortiums, like the Alliance for System Safety of UAS Through Research Excellence, ASSURE, and its accompanying and training arm ASSURED Safe are qualified, equipped, and ready to address these challenges that are affecting the National Airspace System.

[The prepared statement of Dr. Wallace follows:]

20

Testimony

Of

Dr. Ryan Wallace
Professor of Aeronautical Science
Embry-Riddle Aeronautical University

Before

The United States House of Representatives
Committee on the Judiciary
Subcommittee on Crime and Government Surveillance

Unmanned and
Unchecked: Confronting the Rising Threat of Malicious Drone Use in America

Washington, D.C.
September 16, 2025

INTRODUCTION

Chairman Biggs, Ranking Member McBath, and other distinguished committee members, thank you for the opportunity to testify on the important issue of protecting our nation from the misuse of unmanned aircraft systems, sometimes referred to as UAS or more colloquially as "drones."

My name is Ryan Wallace, and I currently serve as a professor at Embry-Riddle Aeronautical University. For the past 10 years, my research has focused primarily on UAS safety and security threats through the use of UAS detection equipment, supported by methodologies such as geospatial analysis and data analytics.

The misuse of unmanned aircraft is not fundamentally a technology problem, but rather a *people* problem. What makes this problem particularly challenging is the unique aerial capabilities that UAS provide to operators—capabilities previously limited only to those with the resources and training to operate manned aircraft. The accessibility, affordability, and automation have now placed these capabilities within reach of anyone with a few hundred dollars. This creates a disproportionate, force-multiplier for bad actors. The destructive potential of consumer drones recently came to global attention in Ukraine during the famed Operation "Spider's Web," where small unmanned aircraft were surreptitiously smuggled into Russia to conduct rapid, surprising, accurate, and devastating attacks against strategic military aircraft. These attacks were executed with near impunity, highlighting the critical vulnerability gap posed by UAS threats. The remote nature of such attacks left no one to arrest or hold accountable.

BACKGROUND

As of the end of 2024, the Federal Aviation Administration (FAA, 2025b) estimated there were more than 2.8M UAS in the United States, comprised of nearly 1.9M recreational UAS and 966,000 non-recreational UAS. Today, drones outnumber manned aircraft by nearly 13-to-1 (Bureau of Transportation Statistics, 2025). Within five years, the agency estimates the total number of UAS will grow by more than 10% (FAA, 2025b).

Drone users can be broadly categorized into five groups: the *compliant*, the *clueless*, the *careless*, the *criminal*, and finally, those *committed* actors intent on using UAS as a weapon for terrorism or causing public harm. I want to talk briefly about each of these groups and reiterate that it is not the UAS itself that causes harm, but rather the people behind these acts. The UAS is merely a tool—one that can be used for constructive or destructive purposes.

The vast majority of UAS operators fall into the compliant category and do their best to follow the rules. Compliance with UAS is a complex endeavor, as the pace of regulatory change, coupled with multiple layers of UAS rules imposed by federal, state, and local governments, makes complete compliance challenging. This important group, however, include the constituents who make up entrepreneurs using drones to advance American business, local governments leveraging drones to improve policing and public safety, and hobbyists pursuing harmless recreation.

The second group is the *clueless*—UAS operators who are unaware of rules or restrictions. These individuals view UAS as a toy, rather than a regulated aircraft that requires knowledge and compliance with rules designed to protect the safety and security of our skies and those on the ground. While

efforts have been taken over the years to improve outreach and awareness, these efforts are being met with varying degrees of success.

The third group comprises the *careless*—these operators are aware of UAS rules and regulations, yet electively ignore them and fly with impunity, in spite of potential risk or consequence. One measure of clueless and careless activity is UAS sighting reports, which include observations of UAS by aircrew members, air traffic controllers, law enforcement, and members of the public, often in areas where they are not permitted to be, or performing activities deemed by the observer to be unsafe. While this measure is imperfect, as it relies on human perception, it does provide a barometer of the state of potentially unsafe UAS activity within the National Airspace System. As of the second quarter of 2025, the FAA recorded a total of 1,022 sightings—approximately 170 per month—with most of these occurrences generally correlating with population centers (FAA, 2025a; Scallon & Wallace, 2025). Of these events, aircrew reported taking evasive action in approximately 2.8% of cases in 2025. The potential consequences of careless operations erode the safety of our skies. As an example, in January of this year, a Canadair CL-415 collided with a Da-Jiang Innovations (DJI) Mini, a 249g drone, operating at low altitude within a temporary flight restriction zone near the Palisades fire. The drone penetrated the aircraft wing, grounding the critical firefighting asset during the height of the incident. Air operations were briefly suspended, allowing the fire to expand unabated, further enhancing the destruction and risk to response personnel (Wallace, 2025).

The fourth group comprises *criminal* use of UAS. While entrepreneurs recognize the value and opportunities that unmanned aircraft bring to business, these advantages are not lost on the criminal elements of society, who also seek technological advantage. As UAS are adept at bypassing ground-based physical security measures, public safety personnel are currently struggling to contain two particular criminal applications of UAS—prison incursions and cross-border contraband delivery.

A 2020 report released by the Department of Justice Office of Inspector General (DOJ OIG, 2020), identified UAS as an increasing threat posed to federal correctional institutions, identifying a substantial uptick in drone incidents at the organization's 122 facilities following the implementation of mandatory drone incident reporting requirements in 2018. In subsequent testimony furnished to the Senate Committee on the Judiciary, Christopher Hardee from the Department of Justice Office of Law and Policy and Michael Torphy, Unit Chief of the Federal Bureau of Investigation's Critical Incident Response Group, cited that drone activity has proliferated to more than half of the Bureau of Prisons federal facilities, with incidents climbing to more than 479 in 2024—nearly 20 times the number since the agency started tracking drone incidents in 2018.

In Georgia, a 2024 joint investigation by the state department of corrections and the FBI thwarted what was described as "a sophisticated, multi-state criminal enterprise" which employed drones as a key tool for injecting contraband into correctional facilities (Kemp, 2024). Law enforcement personnel seized more than 87 drones, 22 weapons, 453 cellular phones, and more than 315 pounds of tobacco and narcotics (Kemp, 2024).

Mr. Steven Willoughby from the Department of Homeland Security highlighted the extent of porous UAS activity along the U.S. border. "In the last six months of 2024, over 27,000 drones were detected within 500 meters of the southern border…" (Willoughby, 2025, p. 2). The operational behaviors of these flights suggest a concerted effort to employ tactics designed to evade customs and border protection agents, such as operating during the hours of darkness, flying above 400 feet above ground level (AGL),

making drones difficult to visually detect, and even conducting counter-surveillance flights against Customs and Border Protection (CBP) personnel.

The final group comprises those who are *committed* to using UAS to cause harm. In 2024, reports emerged that Mexican cartels began employing drones to drop explosives, killing several soldiers in Michoacan (Price, 2024). In August 2025, reports emerged suggesting a drone had been used as a part of a coordinated attack by a Colombian narcotics trafficking gang to down a Colombian National Police UH-60 Black Hawk helicopter, killing all 12 aboard (Forero, 2025; Altman & Rogoway, 2025). While details about this latest incident are still scarce, evidence strongly suggests non-state actors are adapting battlefield drone tactics to great effect, with one source reporting cartel members fought in the Ukrainian theater specifically to gain experience in first-person view (FPV) drone warfare tactics (Altman, 2025).

CURRENT GAPS

I want to differentiate two foundational functions of addressing unauthorized and malicious UAS activity: 1) detection, tracking, and identification (DTI) enabling early warning, airspace situational awareness and monitoring, and risk-driven response decision-making; and, 2) "counter-UAS" often referred to as *mitigation*, which refers to a system or device used to disable, disrupt, or seize control of a UAS (49 U.S.C. §44801[5]). Effective employment of these functions requires three critical components: 1) an understanding of protection priorities and the threat landscape; 2) collection of valid and reliable data derived from tested and resilient DTI equipment; and, 3) efficient application of Rules of Engagement, procedures, or equipment to respond to or mitigate a potential aerial threat.

To effectively address these challenges, I offer several observations—foremost, that all drone incidents are local incidents first. Often, the first response to these incidents will be sworn officers from one of the nation's 17,541 state and local law enforcement agencies (Gardner & Scott, 2018). Most of these agencies lack formal training for dealing with drone incidents, and even fewer are equipped with tools to support the detection, tracking, and identification of UAS. Currently, no state or local law enforcement agencies are equipped and authorized to forcibly take down a UAS threat without the compliance of the operator, who may be positioned miles away from the aerial vehicle. For DJI-manufactured consumer-grade drones, which continue to see heavy use across the National Airspace System, operating range can be five or more miles. Without Remote ID or UAS detection equipment capable of locating the operator, this prospect can be extremely challenging. While the Preventing Emerging Threats Act enabled UAS mitigation authority under relatively tight controls for both the Department of Homeland Security and the Department of Justice, the threat landscape in recent years has changed. When this authority was initially passed in 2018, the FAA estimated the size of the UAS fleet to include approximately 277,000 non-recreational UAS and 1.25M recreational UAS—approximately half the number of UAS estimated to be in active operation today. Similarly, the demand for counter-UAS protection has also increased. Testimony by Michael Torphy from the FBI underscored resource limitations in providing counter-UAS protection to special events, highlighting that the agency was only able to cover 0.05% of the more than 240,000 special events eligible for counter-UAS protection under §124n (Hardee & Torphy, 2025). Ultimately, the widespread, immediate need for counter-UAS protection and available capacity for that response should be part of the calculus used to determine future authorities.

Training is a vital element in preparing our public safety personnel to respond effectively to drone incidents. Foremost, it is essential to ensure that both UAS detection and mitigation efforts do not

create or exacerbate hazards within the National Airspace System through spectrum interference with navigation or communication infrastructure, create collision hazards, or impede air traffic management functions. Second, training is necessary to educate officers on how to effectively respond, investigate, document, and charge these incidents in a manner that leads to successful prosecutions. Moreover, such training ensures reinforcement of appropriate procedures designed to protect rights to expression, privacy, and other civil liberties.

In addition to preparing and equipping public safety personnel to respond to drone incidents, it is critical to ensure access to a consolidated database of nationwide drone incidents. Two such incidents follow, as examples. In 2025, U.S. Immigration and Customs Enforcement removed Fengyun Shi, a Chinese citizen residing in the U.S. on a student visa, following a conviction for using a small UAS to photograph vessels and shipyard infrastructure at two naval facilities near Norfolk, Virginia (Immigration & Customs Enforcement [ICE], 2025; Pearson, 2024). Shi had traveled to Virginia while on leave from his graduate program in the Midwest U.S. (Pearson, 2024). This comes on the heels of another similar incident in late 2024, where Yinpiao Zhou, a Chinese national, flew a small UAS, at altitudes of more than a mile above ground, over Vandenberg Space Force Base inside restricted airspace during a nighttime active satellite launch operation (Brading, 2025; McEvoy, 2024). An investigation by the Air Force Office of Special Investigations uncovered additional photos of sites in Texas, Arkansas, and China (Brading, 2025). Zhao also posted messages on social media seeking ways to bypass UAS altitude limitations (Brading, 2025). The creation of an incident database is likely to improve the ability to detect suspicious cross-jurisdictional activity involving drones. To further support drone incident tracking and streamline information-sharing between agencies, it is also recommended to implement standardized agency reporting nomenclature.

To further reinforce community resilience for drone incidents, public safety personnel require current information about adversary applications and tactics. Understanding technical details of how UAS are tactically employed for various illicit activities enables law enforcement to better identify potential drone threats, determine likely capabilities (such as payload capacity and speed), better assess overall risk, and evaluate effective mitigation and response options. As evidenced in the conflict in Ukraine, the use and tactics of drones are evolving at a breakneck pace, and these lessons are quickly proliferating closer to our borders. Mexican cartels are leveraging small, cheap commercial-off-the-shelf drones and adapting them for surveillance and precision-bombing using rudimentary improvised explosive devices (Villegas, 2025). Devices seized in two Mexican states show continued progression in drone weaponization, including fragmentation munitions, anti-personnel explosives, and chemical devices (Campbell, 2025). Evidence also suggests cartels are adopting strategies to reduce visibility, electronic signatures, and radar footprint of drones through the use of strategic selection of construction materials, UAS design, and adaptive operational tactics (Researching Ukraine, 2025).

There are no “magic bullet” technological solutions to either UAS detection, tracking, ID, or mitigation. Each type of technology has inherent capabilities and limitations. Acquisition of these technologies requires strategically balancing detection effectiveness, accuracy, coverage, ID capabilities, and the ability to locate the operator, all while considering cost. If mitigation systems are also used, careful attention must be given to ensuring adherence to established mitigation legal authorities. The potential for adverse collateral effects should also be considered, which may include spectrum disruption, falling debris, or downrange impacts.

Finally, I would like to highlight the vital importance of continued research and development in this space. Research consortiums like the Alliance for System Safety of UAS through Research Excellence

(ASSURE) and its accompanying training arm, ASSUREd Safe, are qualified, equipped, and ready to address the evolving challenges affecting National Airspace System safety and security, thereby enabling continued progression toward the full integration of advanced aviation technologies.

Thank you for the opportunity to testify before you today.

Acknowledgements

Preparation of this testimony was supported by a number of individuals who provided expertise, analysis, policy recommendations, and related assistance. Acknowledgement does not necessarily imply endorsement of the provided testimony.

Mr. Charles Werner, DRONERESPONDERS
Mr. Mike Monnik, DroneSec
Dr. Jon Loffi, Oklahoma State University
Dr. Anthony Galante, Embry-Riddle Aeronautical University
Prof. Tim Ehrenkaufer, Embry-Riddle Aeronautical University
Mr. Matt Smith, Embry-Riddle Aeronautical University

Ms. Sang-A Lee, Ph.D. Student & Graduate Research Assistant, Embry-Riddle Aeronautical University
Mr. Chris Sidor, Graduate Student, Embry-Riddle Aeronautical University
Ms. Claire Lebakken, Graduate Student, Embry-Riddle Aeronautical University
Ms. Amy Martin, Undergraduate Student, Embry-Riddle Aeronautical University
Mr. Tyler Johnson, Undergraduate Student, Embry-Riddle Aeronautical University

References

Altman, H. (2025). Cartel Members Fought in Ukraine to Learn FPV Drone Skills: Report. *TWZ.* https://www.twz.com/news-features/cartel-members-fought-in-ukraine-to-learn-fpv-drone-skills-report

Altman, H. & Rogoway, T. (2025). Columbian Black Hawn Downed by Drone is a Glimpse of What's to Come (Updated). *TWZ.* https://www.twz.com/air/colombian-black-hawk-downed-by-drone-is-a-glimpse-of-whats-to-come

Brading, T. (2025). Chinese National Sentenced Following Drone Flight During Restricted Launch. *Air Force Office of Special Investigations.* https://www.osi.af.mil/News/Article-Display/Article/4174084/chinese-national-sentenced-following-drone-flight-during-restricted-launch/

Bureau of Transportation Statistics. (2025). Number of U.S. Aircraft, Vehicles, Vessels, and Other Conveyances. *Author.* https://www.bts.gov/content/number-us-aircraft-vehicles-vessels-and-other-conveyances

Campbell, S. (2025). Are We Training for the Right War? *The Zero Lux.* https://www.thezerolux.com/are-we-training-for-the-right-war/

Collett-White, M., Dutta, P.K., & Zafra, M. (2025). How Ukraine Pulled Off an Audacious Attack Deep inside Russia. *Reuters.* https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES-RUSSIA/mypmjzayyvr/

Department of Justice, Office of the Inspector General. (2020). Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prison Facilities Against Threats Posed by Unmanned Aircraft Systems (Report #20-104). *Author.* https://oig.justice.gov/sites/default/files/reports/20-104.pdf

Federal Aviation Administration. (2025a). Drone Sightings Near Airports. *Author.* https://www.faa.gov/uas/resources/public_records/uas_sightings_report

Federal Aviation Administration. (2025b). Compendium to FAA Aerospace Forecast FY 2025-2045: Emerging Aviation Entrants Unmanned Aircraft Systems and Advanced Air Mobility. *Author.* https://www.faa.gov/data_research/aviation/aerospace_forecasts/2025-uas-and-aam-full-document.pdf

Forero, J. (2025). Police Helicopter Downed by Drone in Columbia, Killing 12. *The Wall Street Journal.* https://www.wsj.com/world/americas/police-helicopter-downed-by-drone-in-colombia-killing-12-48117a0d?reflink=desktopwebshare_permalink

Gardner, A. & Scott, K. (2018). Census of State and Local Law Enforcement Agencies. *Bureau of Justice Statistics.* https://bjs.ojp.gov/library/publications/census-state-and-local-law-enforcement-agencies-2018-statistical-tables

Hardee, C. & Torphy, M. (2025). *Securing the Skies: Law Enforcement Drones and Public Safety*. Committee on the Judiciary of the U.S. Senate. https://www.judiciary.senate.gov/imo/media/doc/94f53245-d172-92ba-152b-06bc9ee00a50/2025-07-22%20-%20Testimony%20-%20Torphy%20&%20Hardee1.pdf

Immigration & Customs Enforcement. (2025). ICE Removes Chinese National Convicted of photographing Military Installations. *Author.* https://www.ice.gov/news/releases/ice-removes-chinese-national-convicted-photographing-military-installations

Kemp, B.P. (2024) Gov. Kemp: Georgia Department of Corrections Investigation Exposes Multi-State Criminal Enterprise [Press Release]. *Author.* https://gov.georgia.gov/press-releases/2024-03-28/gov-kemp-georgia-department-corrections-investigation-exposes-multi-state

McEvoy, C. (2024). Northern California Man Arrested for Allegedly Flying Drone Over and Photographing Vandenberg Space Force Base. *United states Attorney's Office.* https://www.justice.gov/usao-cdca/pr/brentwood-man-arrested-allegedly-flying-drone-over-and-photographing-vandenberg-space

Pearson, J. (2024). The Unusual Espionage Act Case Against a Drone Photographer. *Wired.* https://www.wired.com/story/fengyun-shi-espionage-act-drone-photography/

Price, S. (2024). Drug Cartels Using Bomb-Dropping Drones have Killed Mexican Army Soldiers: Report. *Foxnews.* https://www.foxnews.com/world/drug-cartels-using-bomb-dropping-drones-killed-mexican-army-soldiers-report

Researching Ukraine. (2025). Lessons from the war in Ukraine—Coming to a Drug Cartel Near You. *Author.* https://researchingukraine.substack.com/p/lessons-from-the-war-in-ukraine-coming

Scallon, N., & Wallace, R. (2025). UAS Sightings Report Power BI Tool. https://commons.erau.edu/db-aeronautical-science/6

Villegas, P. (2025). With Drones and I.E.D.s, Mexico's Cartels Adopt Arms of Modern War. *New York Times.* https://www.nytimes.com/2025/09/01/world/americas/mexico-cartel-weapons.html

Wallace, R.J. (2025). Why the Super Scooper Wildfire Aircraft Drone Collision Should be a Wakeup Call to the Drone Industry. *Drone Life.* https://dronelife.com/2025/02/11/drone-incidents-involving-aircraft-should-be-industry-wakeup-call/

Willoughby, S. (2025). Securing the Skies: Law Enforcement, Drones, and Public Safety [Testimony before the Committee on the Judiciary, U.S. Senate]. https://www.judiciary.senate.gov/committee-activity/hearings/securing-the-skies-law-enforcement-drones-and-public-safety

Mr. BIGGS. Thank you, Dr. Wallace. Now, the Chair recognizes Dr. Cahill for her five minute opening statement.

STATEMENT OF DR. CATHERINE F. CAHILL

Dr. CAHILL. Thank you. Chair Biggs, Ranking Member Raskin, and Ranking Member McBath, and the esteemed Members of the Subcommittee on Crime and Federal Government Surveillance. My name is Cathy Cahill, and I'm the Director of ACUASI, the Alaska Center for Unmanned Aircraft Systems Integration.

The ACUASI leads one of the seven FAA test sites where we are a key player in many other FAA, DOJ, and DOD programs. We also partner with a variety of commercial and governmental entities on cutting edge UAS and counter-UAS technologies, required to safely integrate UAS us into the National Airspace System. These facts uniquely position me to discuss the topic of malicious UAS. This written testimony is provided to you through my personal capacity as a private citizen based on my professional experience. It does not necessarily represent the views of the University of Alaska.

The ACUASI uses UAS for good, such as conducting medical supply delivery, cargo delivery to isolated communities, and emergency response. However, our team is very aware of how they can be used maliciously.

I live in Alaska, but even in this remote location our team has seen the malicious use of UAS. We have seen flights of unauthorized UAS in the flight path of Ted Stevens International Airport, one of the top five cargo airports in the world.

Simultaneously, we have seen multiple UAS entering restricted airspace of our military bases. We have observed the flight tracks of UAS dropping contraband into correctional facilities. I personally have seen UAS crossing the Southern border, bringing drugs from Mexico. All these examples show the malicious UAS activities are widespread, and we need policies, procedures, training, and technologies to allow law enforcement to stop these activities without creating a hazard to people and property.

The first question I always get asked when I talk to the public about the issue of malicious UASs, why can't we shoot them? The United States Code, Section 49, defines UAS as aircraft and all the laws codified for traditional manned aircraft apply to them. Therefore, shooting an UAS is a Federal offense with applicable jail time and fines. Only five agencies, DOD, DOE, DHS, DOJ and, to a limited extent, FAA have relief from the United States code sections applicable to shooting down, hacking, or jamming UAS. Most law enforcement operators dealing with unauthorized UAS do not have the legal authority to do so. Also, it is unsafe to mitigate a UAS without knowing what is under it and one might get hit when the UAS falls.

Additionally, the operator of a counter-UAS system needs to know that UAS under operation is authorized to be flying in that location. These facts point to why we need highly trained professionals with appropriate statutory relief and good information, making the risk benefit calculations about whether and how a UAS should be mitigated.

As the malicious use of UAS spreads, State, local law enforcement, and officers will be on the front lines for combating the threat from the rogue UAS, because Federal agents with counter-drone capacities cannot be everywhere. The ACUASI team has been studying the willingness of local law enforcement officers to engage with systems designed to detect, track, and identify malicious UAS.

In Alaska, we have had trouble getting State and local law enforcement officers to address rogue UAS because they are overworked, understaffed, dealing with more urgent situations, and feel it is not their responsibility to do so. Additionally, many of the law enforcement participants in our study aren't sure as to what laws are applicable to malicious UAS, and do not know what they can legally do to build a case for the misuse of UAS.

We need to provide our law enforcement officers with clear guidance on how to address rogue UAS. As the risk from malicious UAS increases, the potential to mitigate the UAS is certain circumstances.

We cannot afford to allow criminals to use UAS maliciously, or our adversaries to use UAS to endanger our military bases or personnel and conduct espionage. In my opinion, H.R. 5061, the Counter-UAS Authority Security, Safety, and Reauthorization Act is a good first step toward safely implementing counter-drone technology in the U.S. However, more needs to be done.

To accelerate our testing and implementation of these technologies and the required risk benefit decision calculations needed before UAS is mitigated. These investments will not only help our law enforcement organizations here at home, but also our military overseas, as they deal with the malicious UAS threat.

The U.S. should be a world leader in the development and deployment of these technologies. If we do not move fast enough, the criminals and our adversaries will win the UAS war.

This ends my prepared statement. I'd be happy to answer any questions you have.

[The prepared statement of Dr. Cahill follows:]

The Written Testimony of Dr. Catherine F. Cahill
Director, Alaska Center for Unmanned Aircraft Systems Integration (ACUASI) at the University of Alaska Fairbanks (UAF)

U.S. House of Representatives Committee on the Judiciary
Subcommittee on Crime and Federal Government Surveillance

Unmanned and Unchecked: Confronting the Rising Threat of Malicious Drone Use in America

September 16, 2025

Chairman Jordan, Ranking Member Raskin, Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee on Crime and Federal Government Surveillance, my name is Cathy Cahill, and I am the Director of the Alaska Center for Unmanned Aircraft Systems Integration (ACUASI) at the University of Alaska Fairbanks (UAF). ACUASI is the University of Alaska's Center of Excellence for Unmanned Aircraft Systems (UAS), also known as drones, and one of the top UAS research programs in the country. ACUASI leads of one of the seven Federal Aviation Administration (FAA) designated UAS Test Sites, heads one of the eight BEYOND Phase 2 sites, and is a core university in the FAA's UAS Center of Excellence (a.k.a. the Alliance for System Safety of UAS through Research Excellence – ASSURE). We also partner with the best and brightest commercial and governmental entities on the cutting-edge UAS and Counter-UAS (C-UAS) technologies required to safely integrate UAS into the National Airspace System (NAS). ACUASI's diverse portfolio, operational expertise, and academic standing allow us to demonstrate, observe, and evaluate the benefits and risks associated with UAS and C-UAS use in both military and civil environments. Combined, these facts uniquely position me to discuss the topic of the use of malicious UAS. This written testimony is provided to you through my personal capacity as a private citizen and based on my professional experience; it does not necessarily represent the views of the University of Alaska.

Unmanned Aircraft Systems (also known as UAS, UAVs, Remotely Piloted Aircraft Systems [RPAS], or drones) have a tremendous potential to increase aviation safety by doing the dirty, dull, and dangerous flights that currently put pilots of manned aircraft at risk. They also can improve public safety and quality of life through delivering cargo to remote areas, accelerating medical supplies deliveries, providing broadband communications to remote areas, improving maritime domain awareness, facilitating Search and Rescue, assisting law enforcement operations, monitoring infrastructure, and conducting a host of other positive uses. However, UAS also can be used to commit crimes, disrupt airports, interfere with commerce and transportation, conduct war, support terrorism, cause fear, and conduct other malicious acts. As a result, the U.S. needs to develop, test, and implement policies and procedures for use by law enforcement organizations and safe C-UAS technologies that will allow for the safe removal of malicious UAS from the skies by authorized individuals to ensure public safety. A key part of the mitigation of malicious UAS will be the training of all authorized operators about applicable laws governing UAS usage and the benefits and risks associated with using C-UAS technologies. This will allow law enforcement personnel to make educated decisions about how to engage with a malicious operator and their UAS.

As the malicious use of UAS spreads, state and local law enforcement officers will be on the front lines for combating the threats from the rogue drones. Therefore, state and local law enforcement officials need to be educated about what laws are applicable when they encounter a UAS operator conducting careless, clueless, or criminal activities and how to safely resolve the situation whether through engagement with the operator or the use of C-UAS technology to mitigate (e.g., stop the UAS activity or remove it from the air). In my opinion H.R. 5061 Counter-UAS Authority Security, Safety, and Reauthorization Act is a good first step towards safely implementing these technologies in the U.S.

Watching the news or conducting a cursory Google search will result in multiple articles describing the malicious use of UAS. Airports have had near-collisions and stoppages due to UAS being flown over and around the airport[1]. UAS are interfering with wildfire fighting and medical evacuation operations[2]. UAS are being used to bring contraband into prisons[3]. UAS are bringing drugs over the U.S. border[4]. UAS are being used to surveille or damage critical infrastructure[5]. UAS are being flown by drunk operators, over people without the proper safety equipment, to ensure security guards are not near a location, etc.

I live in Alaska, but even in this remote location, our team and partners have seen the malicious use of UAS. We have seen flights of unauthorized UAS in the flight path of Ted Stevens International Airport in Anchorage, one of the top five cargo airports in the world, and near other critical infrastructure. Criminals have used UAS to drop contraband at correctional facilities. We have had wildfire fighting and medical evacuations stopped due to UAS violating the Temporary Flight Restriction (TFR) over the fire. One of our team members was cut by a piece of a UAS flown by a drunk operator that hit power lines and broke apart as it crashed. All of these examples show that malicious UAS activities are widespread and that we need policies, procedures, training, and technologies to allow law enforcement to stop these activities without creating a hazard to people and property.

The first question I always get when I talk to the public about the issue of malicious UAS use is, "why can't we shoot them." The answer is not as straightforward as it would seem. First of all, according to the United States Code (U.S.C.) Section 49 defines UAS as aircraft and all of the laws codified for traditional manned aircraft apply to them. Therefore, shooting a UAS is a Federal offense with applicable jail time and fines. Only five Federal agencies (DOD, DOE, DHS, DOJ, and the FAA) have relief from the U.S.C. sections applicable to shooting down or jamming/hacking UAS, so most law enforcement operators dealing with unauthorized UAS do not have the legal authority to do so. Second, unlike shooting a firearm at a target where you can see what your bullet might hit if you miss the target, if you shoot at a UAS, you usually cannot see what is under the aircraft and might get hit by the falling aircraft or its pieces. Third, basic physics says that what goes up must come down, so the bullet you fired into the air could come down on a person or property. Fourth, you may not be looking at a nearby UAS, but a more distant manned aircraft. A study conducted by the FAA Center of Excellence for UAS Research (ASSURE) shows that even trained observers can have trouble telling how far a manned aircraft is from them[6]. This means it is even more difficult to determine the distance of a small UAS from the observer. Additionally, night complicates the whole situation by making the aircraft and UAS more difficult to see. Fifth, you do not know if the UAS you see is authorized to be flying in that location. You would not want to be liable for shooting down an authorized UAS that could be carrying hundreds

of thousands of dollars' worth of camera or sensor equipment. These factors and multiple others mean that a private citizen shooting at a UAS is a very bad idea.

The recent New Jersey 'unauthorized drones' scare, when FAA-approved UAS, distant planes, and other lights in the sky caused citizens to have concerns about terrorist drones, highlighted the fact that there is not a consensus on who should have C-UAS authority[7]. State and local officials and legislators, and many members of the public, wanted state or local entities to be able to use C-UAS to shoot the 'drones'. In my opinion, the risk of unintended consequences from a mitigation attempt by an untrained state or local entity is too high. The primary job of the state or local official will most likely not be C-UAS operations, and they may not have all of the information about the operation of the UAS of concern and the risks of the mitigation attempt.

The good news is that authorized and trained Federal personnel have multiple types of C-UAS mitigation technologies either in use or under development for their use[8]. Due to the physical and privacy risks associated with conducting C-UAS operations, the authority for conducting C-UAS activities has been limited to five agencies (i.e., DOD, DOE, DHS, DOJ, and the FAA). This ensures the highest level of training, oversight, safety, and security while protecting the public, UAS operators, and others from potential collection and misuse of personally identifiable information or adverse impacts from uninformed mitigation decisions. These agency personnel must determine if the risks due to the rogue UAS outweigh the risks associated with the removal of the UAS. In my opinion, some of the mitigation techniques, such as those involving the physical damaging or destruction of the UAS, should remain with the trained agency personnel due to their risks to aviation and people and property on the ground. I am a little bit more comfortable with allowing the mitigation of UAS using non-destructive techniques, such as hacking and jamming, by state and local law enforcement officials, provided they have extensive training about the potential risks of these systems to First Responder communications, aviation navigation systems, and other critical systems. This will require giving the trained personnel relief from the parts of the United States Code pertaining to hacking and jamming systems (e.g. Title 18).

There are also systems that are capable of detecting, tracking, and identifying (DTI) UAS. The track data collected from the systems can be compiled into maps that show the most common launch and recovery points and flight tracks. Law enforcement officials can use this information to determine where to go to observe potential criminal UAS operations and to catch the perpetrators in the act. Some of these DTI systems allow the system's operator to determine the location of the UAS operator. Law enforcement personnel can use the systems to find the operator of the UAS and educate them about proper drone use if they are careless or clueless or arrest them if they are conducting criminal acts. I am very comfortable with granting state and local authorities permission to use DTI systems that have been tested to ensure no adverse side effects to their use.

Remote ID, a legal requirement that the UAS broadcast its location and identification during operation will allow security officials to separate authorized UAS from unauthorized UAS[9]. However most rogue and home built UAS probably will not be broadcasting RID signals or may be broadcasting false signatures, so other forms of DTI will be needed to determine the location of the rogue UAS and its operator. I would be comfortable with granting state and local governmental DTI operators Title 18 relief to get information about the UAS's operator from the UAS if they are not using Remote ID.

The ACUASI team has been investigating the willingness of local law enforcement officers to engage with DTI systems. In Alaska, for example, we have had difficulty getting local and state law enforcement to address rogue UAS because they are overworked, understaffed, feel it is not their responsibility to do it, and do not know what they can legally do to build a case for the misuse of the UAS. Additionally, many of the law enforcement participants in our study are unsure as to what laws are applicable to malicious UAS use. This includes being unclear as to what is allowed under FAA regulations for recreational and commercial UAS use as well as other regulations, such as operating an aircraft while intoxicated. Our law enforcement/C-UAS project manager describes the situation as everyone standing in a circle and pointing at someone else in the circle as being the responsible party. However, we have found that once the officers see a situation in which the DTI system provides a benefit, they are more willing to engage with the system. One example of this was the recent glacial outburst flooding in Juneau, Alaska. The State of Alaska Department of Transportation and Public Facilities put up a TFR over the river so they could monitor the flooding using their UAS. A DTI system was deployed to monitor the TFR. The DTI system captured a UAS violating the TFR and nearly missing a DOT UAS. The system was able to track the UAS back to its launch point. Local law enforcement officers then went house to house in that area and were able to find and engage with the UAS operator. Another example was when a DTI system tracked a contraband drop into an Alaskan Correctional Facility. The facility, which had been skeptical about the use of a system, immediately requested that all of their personnel be trained as quickly as possible.

We cannot afford to allow criminals to use UAS maliciously or careless or clueless UAS operators to endanger U.S. airspace and people and property on the ground. The U.S. needs to invest in: 1) training law enforcement personnel in how to engage with malicious UAS operators, 2) establishing the requirements for a clear chain of custody for evidence of criminal UAS activities, 3) developing clear guidance for law enforcement about applicable laws, policies, and procedures, and 4) DTI and C-UAS technologies. This investment will help not only our law enforcement organizations here at home, but also our military overseas as they deal with malicious UAS. The U.S. should be the world leader in the development and deployment of these technologies; if we do not move fast enough the criminals and our enemies will win the UAS war.

This ends my prepared statement, and I would be happy to answer any questions you might have.

1.https://www.skysafe.io/blog/drones-and-airplanes-a-growing-threat-to-aviation-safety)

2.https://www.justice.gov/usao-cdca/pr/culver-city-man-agrees-plead-guilty-recklessly-crashing-drone-super-scooper

3.https://nij.ojp.gov/topics/articles/addressing-contraband-prisons-and-jails-threat-drone-deliveries-grows)

4.https://www.newsnationnow.com/us-news/immigration/border-coverage/border-patrol-expands-blimp-surveillance-to-combat-drone-threat/#/questions/5662210

5.https://dronelife.com/2021/11/08/drone-attack-on-u-s-power-grid-failed-this-time/

6. https://assureuas.org/wp-content/uploads/2021/06/A46-Final-Report.pdf

7.https://www.faa.gov/newsroom/dhs-fbi-faa-dod-joint-statement-ongoing-response-reported-drone-sightings

8.https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS-Detection-Mitigation-Systems-ARC_Final-Report_02052024.pdf

9. https://www.faa.gov/uas/getting_started/remote_id

About Dr. Cahill:

Dr. Catherine (Cathy) F. Cahill is the Director of the Alaska Center for Unmanned Aircraft Systems Integration (ACUASI) and a Full Professor of Atmospheric Chemistry at the University of Alaska Fairbanks (UAF). Her educational background includes earning degrees in Applied Physics (B.S.) and Atmospheric Sciences (M.S. and Ph.D.) and researching trans-Atlantic aerosol transport during a Fulbright Fellowship to Ireland that served as her Postdoctoral experience. For many years, her research focused on the sources, transport, transformation, and impacts of atmospheric aerosols, including the effects of atmospheric aerosols on the Warfighter in Iraq and Afghanistan and the long-range transport of pollution from China into the Arctic. To understand the altitudes at which pollution crosses the Pacific Ocean, Cathy needed to make vertical measurements of aerosols in the atmosphere. In 2006, this need led her to start designing aerosol samplers for unmanned aircraft. After a 2014-2015 sabbatical to Washington D.C. in which she served as a Congressional Fellow to the U.S. Senate Committee on Energy and Natural Resources, Cathy returned to UAF and became the Director of ACUASI. Since then, she has participated in the FAA's Beyond Visual Line of Sight Aviation Rulemaking Committee and served on the FAA's Drone Advisory Committee/Advanced Aviation Advisory Committee.

Mr. BIGGS. Thank you. I now recognize the Ranking Member of the Subcommittee, Ms. McBath, for her opening statement.

Ms. MCBATH. Thank you, Mr. Chair. Thank you to our witnesses. I have read your testimonies, and I apologize that I am just getting here. Thank you for convening today's hearing to provide us with an opportunity to learn more about how drones can be used to commit crimes; how law enforcement can respond to those crimes; and what we might do here in Congress to adapt our laws to meet the challenges that drones pose to our society and the challenges that you have expressed today.

As with the internet, artificial intelligence, and so many other technologies, drones can really be a valuable tool. They can help first responders that survive or survey a disaster area to search for survivors, or they can give law enforcement another vantage point from which to monitor a special event or a very sensitive location. They can keep officers safe by allowing them to remotely investigate a dangerous situation or location. The rapid proliferation of drone technology has ushered in a new frontier of crime, and many, many public safety challenges.

In the wrong hands, drones can be used to invade privacy, smuggle contraband, as you just mentioned, or provide bad actors with information that can help them avoid detection. I've heard firsthand about these harms from many law enforcement officers, in particular, in my district in the State of Georgia, as they are working to keep us all safe. For example, Georgia prison officials have informed me that they are increasingly battling the use of drones to smuggle contraband into our prison facilities. Drones have been used to deliver illegal drugs, weapons and cell phones, which can each pose a threat to the safety of our inmates and also the staff.

Just last year, the Georgia Department of Corrections see drones, dozens of them, that could be used to smuggle in contraband. Recently, officials at Washington State Prison in Davisboro, Georgia, they worked with the Washington County sheriff to track drones that were being used in an attempt to smuggle methamphetamine and heroin into prison. By tracking the drones and using a K–9 unit, they were able to locate the drone operators, arrest them, and prevent the drugs from reaching the prison.

While law enforcement succeeded in this effort, using traditional tools, additional law enforcement tools may be needed to respond to the rising challenges that are presented by the drones.

As with any new technology, we must exercise caution and proceed thoughtfully to avoid unintended consequences of detecting and mitigating drone activities. Disabling or intercepting drones presents very unique challenges. For example, an intercepted or disabled drone could fall as was stated, and injure innocent bystanders on the ground, damage objects, or property in its path. Similarly, many of the technologies used to combat drones rely on disrupting their communications systems of planes or emergency—these communication systems could disrupt aircrafts or emergency responders.

The testing, planning, training, and targeted deployment can all help ensure that counter-drone technologies are used in a way that promotes public safety, but also strengthens our national security.

I'm so thankful to each of our experts today for your expert testimony. Thank you for coming here today to discuss how we can work together to respond to these challenges and opportunities that have been presented by drones and counter-drone technology and our ever-changing technological landscape. Thank each of you for sharing your expertise.

Mr. BIGGS. The gentlelady yields back. Now, we'll go to questions from Members of the Subcommittee, we'll start first with the gentleman from Texas, Mr. Nehls.

Mr. NEHLS. Thank you, Chair. You spoke so well about the issues that we see down at our Southern border related to drones coming across with all the drugs, killing our people from the bad hombres we have on the Southern border. We have to stop it.

I'd like to talk a little bit about drones in the airspace, specifically airports, concerned about the airports, right? A bad actor with bad intentions, entering restricted airspace over one of our airports. As I do, I am looking at you, I am thinking about Florida. You have about 400 airports as your responsibility. What does a medium-size airport do? You detect at the airport, a drone comes in restricted airspace, what's your response?

Sgt. DOOLEY. Normally, I'll give you an example. We've done some really different things in South Florida, especially Miami International Airport, as an example, has a drone problem and we have partnered with our FAA partners, DHS, et cetera, entities that are allowed without question to detect or mitigate because we recognized it was an issue. We incorporate a lot of our public safety in the area of Miami–Dade, et cetera, and we were involved as well. We are able to go out there and start intercepting, but from the perspective of an airport that simply has the ability to detect and there is really nothing they can do other than watch it, honestly.

Mr. NEHLS. Did you see how stupid that sounds?

Sgt. DOOLEY. It does.

Mr. NEHLS. It's stupid.

Sgt. DOOLEY. Yes.

Mr. NEHLS. I like the idea we can detect; we can detect. All these airports we can detect a drone. Well, if it's being operated by an individual with some bad intentions, you'll just catch it on video. The destruction of—you are going to detect it, but there's nothing to mitigate that drone? This is airports, correct me if I am wrong, sir, but this is airports across the entire country.

Sgt. DOOLEY. Yes, that's correct. There may be some that have specialized, but—

Mr. NEHLS. Well, Ms. Cahill brought up a few of the agencies that have the ability to mitigate a drone.

Dr. Wallace, I hear these arguments, I'm on the Transportation Committee, I hear all these arguments about you can't mitigate the drone because it could interfere, it could interfere with commercial aviation and all this. Is there technology available out there that could mitigate a drone without interfering with our commercial air?

Dr. WALLACE. There are certainly several technologies that are available for mitigation.

Mr. NEHLS. Sure.

Dr. WALLACE. Each of those technologies have their own benefits and limitations.

Mr. NEHLS. Sure, sure. That's an excuse that I hear over and over again, it's going to interfere with the aircraft that are coming in, I said, interfere with the aircraft coming in. The damn drone could take down one of our aircraft. You talked a little bit about what we've seen in Ukraine with the complex missions that some of these drones are taking. I am appalled by the fact that I was in Milwaukee and I went to visit the airport, we were talking about the drones, and I was inside there. I said well, "what happens if a drone gets into this red air—this restricted airspace?" "Well, we know it's there." I said, "what would you do?" "We try to call somebody. Yes, we try to find the guy, he could be a couple blocks, a couple miles away in the backyard and we will knock on the door." I said, "What if that guy has bad intentions?" "Then, when we have a significant event, we'll bring in the Coast Guard. The Coast Guard would have the ability to mitigate the drone and send it out to Lake Michigan or set it down."

The idea to say that, we have to be careful here that the drone doesn't fall down and hit somebody in the head. The technology is there to take control of the damn drone and get it out of the restricted airspace. The idea that we have to be worried about not offending somebody; it's in restricted airspace. At some point in time, Mr. Feddersen, we're going have a drone operated by some bad hombres over here interfering with some commercial airliners, running into the engines and causing problems but then, maybe then, is when we will actually get serious about mitigating the risks of these drones, because there's going to be millions of them out there. The bad guys are understanding these are pretty—you can put some pretty good payload on some of these drones, they are relatively inexpensive, right? So, I am deeply concerned, Sergeant Dooley, about the U.S. Government's position on this, whether it is Section 49, it is a Federal offence, that just makes me sick to think that this is a Federal offense for State individuals, State officials to protect their own airports in their own State. We must change; we must change.

I yield back.

Mr. BIGGS. The gentleman yields. We appreciate that. The Chair recognizes the gentlelady from Georgia, Ms. McBath.

Ms. MCBATH. Thank you so much, Mr. Chair.

We know that drones, as I've stated and many have stated in this hearing, drones have been used to smuggle drugs, weapons, and phones into prisons and across our borders. As I mentioned in my opening remarks, this is already happening in Georgia. Drones present a significant risk to the safety of inmates and staff.

Dr. Cahill, your written testimony notes that your team has worked with Alaskan correction facilities to detect and to track and to identify the drones that are being used to smuggle contraband into the prisons. You also said this is a widespread problem, but can you talk about—you said that you had difficulty in getting law enforcement to address the rogue UAS, and so including at correctional facilities. Could you explain the source of the hesitancy?

Dr. CAHILL. Ranking Member, the reality is when we have dealt with our law enforcement, they are skeptical of a new technology

until it is proven because they have so many things on their plate that it is a challenge for them to learn something new and be able to work with it. We had hesitancy in our correctional facilities for installing one of these systems. The moment we did and were able to confirm some of their intelligence that there was a contraband drop occurring and we were able to track the drone, identify where the hand controller for the operator was. We changed their opinion. As soon as we gave them that briefing the answer was: Could you please train us this afternoon? We did.

They've spread that story to additional correctional facilities and they've accepted it. They have a very targeted, very limited area that they need to protect.

The police and the Alaska State troopers who have much wider ranges for them. We are severely understaffed. So, a malicious drone doesn't mean anything compared to wife beating or major traffic accidents in the middle of nowhere. The priority is not there to be able do these additional duties associated with monitoring the technologies and determining how to interact with them.

Ms. MCBATH. Could you kind of explain to me when the drones are seized in these crimes, what type of digital forensics can be performed on them? What data can be extracted or recovered from a seized drone?

Dr. CAHILL. The Ranking Member, we don't actually do the forensics on the drones. People do, for example, the Pacific Palisades case where the drone hit the Super Scooper, a fire-fighting aircraft. They were able to do a forensic analysis because the drone was stuck in the wing of aircraft. In a lot of these cases, all we see are the tracks and we may know it is group one or group two, which is the size category, but we don't know a whole lot about that aircraft because we have to obey Title 18 and Title 49, which means we cannot break into the communications link for that aircraft without permission, the 124 and authority, for example. We as a State university do not have that, but the partners we have who do, they are able to get more information in terms of what the serial number is what type of aircraft it is. They can say it is a DJI Mavic, for example. It really is a function of what you have.

What we are doing when we are using passive RF is for trying authorization, is we are looking for basically somebody yelling. We have a network of censors, and we determine the direction from which the yelling is coming. That lets us find the drone and the operator. We will be able to track where the drone is and where the operator is. In the recent case with the Juneau glacial outburst flooding, we said at the system we were able to determine where the controller was, where the drone went and landed, local law enforcement went to that location and knocked on doors and found the perpetrator.

Ms. MCBATH. Then, would you say that local law enforcement is able then to build a criminal case from the data that they are to extract that you can't do it but they can?

Dr. CAHILL. Yes.

Ms. MCBATH. OK, thank you. Sergeant Dooley, what are the greatest legal and technical hurdles in actively encountering a drone in real time?

Sgt. DOOLEY. Just to the doctor's point again, we do have legal constraints, we would violate about 15 different U.S. codes by simply frequency jamming or mitigating all kinds of FAA rules, regulations, FCC, et cetera. Most of those carry jail time and significant fines as well. A lot of colleagues would say, "Like, oh, well, we're public safety, if we have to do what we have to do." The problem is, to your point earlier, mitigating a drone and they may have had a legal right to be there, and they made an honest mistake, there is still a tremendous amount of consequence that comes with that.

Our biggest hurdles are all the existing codes, our laws simply do not keep up with the rate the technology progresses, and the way that it can be manipulated for bad. Those are some of the biggest hurdles we have is Title 18 pen trap, wire-tapping laws, et cetera, that are of huge concern when we do want to not only detect that a drone is there, but be able to mitigate it away, we would be violating about 15 different title codes, and also Title 18 and 49 as well.

Ms. MCBATH. Thank you. I appreciate it.

Mr. BIGGS. The Chair now recognizes the gentleman from Wisconsin for five minutes, Mr. Tiffany.

Mr. TIFFANY. Thank you, Mr. Chair.

As we heard over the last few years, every State became a border State, with the previous administration and cartel members openly stated that they used our Northern border to smuggle in narcotics. Mr. Feddersen, do you think it is equally important to implement these drone enforcement programs at both the Southern border and the Northern border?

Mr. FEDDERSEN. Yes, sir, I do. They are being implemented at the Federal level, particularly CBP on both the North and the South sides. However, the lack of authorities for detection track identifying, or even the mitigation piece does extend to those local departments that are shoulder to shoulder with CBP taking action to address these issues. We are severely overmatched by the criminal element when it comes to it.

Mr. TIFFANY. How should that change in your opinion?

Mr. FEDDERSEN. It is actually quite easy, sir. Detect, track, and identify authority is our Title 18. They are very vague, they are antiquated, and they honestly add a lot of confusion to law enforcement, commercial sectors, and critical infrastructure that want to be able to see what's flying in their airspace. The information that goes from there into the counter-drone systems like ours are nothing more than remote ID data. It's just data that comes directly from the drone. The most personal information you may get from it is the serial number which is akin to license plate on a vehicle. Law enforcement still has to call the FAA to get the registry information from the FAA and then from there, be able to take leaps.

The DTI should be a blanket open authority for critical infrastructure, security, law enforcement and honestly, all Federal agencies because they don't all have the authority right now.

Mr. TIFFANY. With that authority they could accomplish the mission that you were referring to that they are not able to fulfill at this point. Is that correct?

Mr. FEDDERSEN. Correct, most of it, because at this point, you can figure out where the drone is, where it took off, and where the pilot is in real time.

Mr. TIFFANY. The cartels and others are light years ahead of the law enforcement at this point in part because of that?

Mr. FEDDERSEN. Honestly, the rest of the world, sir. We are a global country in 33 countries. We do airports and law enforcement and military everywhere else, and they use our system quite a bit to mitigate.

Mr. TIFFANY. Mitigation looks much different in other places around the world than it does here in the United States?

Mr. FEDDERSEN. It is only the policies and legislative piece. They have given authorities to their law enforcement and security entities.

Mr. TIFFANY. You think China may have had a hand in the drone activity around some of our military sites?

Mr. FEDDERSEN. Yes, sir, absolutely. I believe that drones are a tool, they are a tool by criminal networks, and they are a tool for foreign adversaries. Absolutely, they are being used.

Mr. TIFFANY. Sergeant Dooley, are you familiar with the Guang Pan Cape Canaveral incident that happened earlier this year in Florida?

Sgt. DOOLEY. Vaguely, yes.

Mr. TIFFANY. In the case of Chinese-born Canadian citizen Guang Pan was found to be using a drone to take unauthorized photographs at Patrick Air Force Base, a submarine morph in Cape Canaveral. Have you seen increased activity of drones around U.S. military bases in Florida?

Sgt. DOOLEY. Military bases not so much. We don't support them as often, it is normally during large scale events, but we went from literally detecting a few hundred per month in those general areas where they are restricted airspace like a DOD site or a military base to thousands. In particular, when DGI, in particular, drones, turned off their geofencing for the most part. Our principal workhorse years ago in the State of Florida, what we used was DGI drones. That is how we got started. Now, we are not allowed to use them anymore. Back then, you had to have special permission, the drone told you, you're not allowed to fly here or take off from here. Now, that is not the case. It is simply a check box where you turn on your drone and it can be right next to an airport runway, and before it would say, "You can't fly here." It says, you're taking responsibility, you touch a check box and it takes off and flies wherever I want it to fly now. We've seen dramatic increase over the past, I would say, 8–9 months of going from a handful of detections to in the thousands of detections in these areas or within range of our detection equipment because there is no more geofencing. Yes, it has increased dramatically in a lot of these areas, not just for infrastructure, but our military sites and other places.

Mr. TIFFANY. Is it correct that we do not produce a lot of drones in the United States principally produced in China. Is that accurate?

Sgt. DOOLEY. That's correct. The principal ones that are produced here are normally purchased by DOD or law enforcement or areas

like Florida where we restrict the type of drones we're allowed to purchase.

Mr. TIFFANY. For national security purposes, do you think that we should make that a priority to be able to produce them in the United States?

Sgt. DOOLEY. I am a proud American for sure; I would love to be prideful of us producing those types of things here, yes. I also don't want to stifle some of the things where people need to buy a certain product because it is the correct tool for the correct job if that makes sense, but buying American should be preferred, yes.

Mr. TIFFANY. Thank you, Mr. Chair. I yield.

Mr. BIGGS. The gentleman yields back. Before we go to the next one, I want to submit for the record documentation called, "Cartels Drop Bombs From Drones Near Southern Border." So ordered.

I recognize the gentleman from California, Mr. Swalwell, for five minutes.

Mr. SWALWELL. Thank you. There's no doubt that drones particularly for law enforcement have changed the game for surveillance, for search and rescue, to assist in active SWAT operations, they can save not only civilian lives, but also protect our men and women in law enforcement. The Sergeant just alluded to a problem that we have run into is that cheaper Chinese components have made it much more affordable for law enforcement agencies to have these capabilities. We all know the risk that comes along with having Chinese components in our drones, which is that they could be pinging back to mainland China and affecting our own national security in the way that they could be gathering intelligence on behalf of the Chinese Government. Certainly, no law enforcement agency wants that.

Sergeant Dooley, I imagine you would tell me that when you're making decisions to protect the people who work with you and to protect the public, you have to think about what can bring public safety and how you can stretch your dollars the best. Is that right? Is that some of the tension you have to deal with in making a decision like that?

Sgt. DOOLEY. Not anymore. The State of Florida legislated that, so we don't have to worry about it, we just take what we need. They also supply funding now to help us reach those goals of transitioning everything away.

Mr. SWALWELL. My goal, just as you stated earlier, is that we would have entirely an affordable American-made supply chain. In fact, in California, there's a company, it's made up of former Navy SEALS, called Inspired Flight which is American made components. It sounds like you're familiar with Inspired Flight.

Sgt. DOOLEY. Oh, yes. They are good people. I like them.

Mr. SWALWELL. Yes, same. My question for Dr. Wallace is knowing that 86 percent of the drones—I'm sorry. Knowing that a high percentage of drones are made in China, in that the over concentration can affect our national security. What can we do in the near term to make sure that law enforcement has affordable drones, but on the manufacturing side that we're able to expedite our ability to produce American made components?

Dr. WALLACE. That's an excellent question. I can tell you, I'm not a manufacturing expert. I can tell you that from a capabilities' per-

spective, currently Chinese made drones have a capability that can't be matched with the same dollar value. I do think that given that limitation the choice that ultimately has to be made with regard to especially public safety is one of lives, because at the end of the day, if public safety agency doesn't have access to the tool they need to protect that public and the capability they need to accomplish what they need to do, the ultimate price will be either law enforcement member's life or potentially a member—a citizen's life. That is a metric that should be taken?

Mr. SWALWELL. Agreed. Sergeant Dooley, are there any examples you have not given the Committee as to how a drone facilitated saving life or protecting the officers who worked with you that you think could animate the need for giving law enforcement more resources in this area?

Sgt. DOOLEY. For the counter site or just a success story from having drones in public safety?

Mr. SWALWELL. Both.

Sgt. DOOLEY. OK, from the success side, I will give you an example and I give it all the time, I work very closely with the Palm Beach County sheriff's office in South Florida. There was a deputy and I were eating lunch and we get this call of a stabbing inside a home and everybody fled. Unfortunately, the person that was the criminal in this particular case was off his medication, recognizing that we may have had some type of mental episode and we approach it differently. As soon as we arrive there, the deputy get permission to put his drone and I supported him by making sure everything was squared aware. He put his drone under the house and within three minutes he located the suspect, we recovered the suspect, they are in custody, no one got shot, not one got dog bit. Everybody went on about their day and the person who had been stabbed was getting medical attention. This was solved in minutes, versus like an hour standoff with a SWAT team without this type of technology.

From the other side of not having detection or counter UAS that has been hindering is a bulk of what we get is like careless and clueless individuals where they just as dangerous at times as someone with bad intent. For example, the person in California gave an example of hitting the sea plane that was—I forget the name of it. That person didn't do it on purpose; they were just careless and clueless. Same thing in Texas during the flooding, we had someone strike a helicopter. They didn't do it on purpose, sometimes careless and clueless individuals, dangerous as those that have those negative intentions. Having this technology both for public safety provides a tremendous value of being able to save lives, to protect lives. More importantly, having the ability to detect and potentially mitigate if needed could provide those values where we can keep mandate aviation safe. We harp on the terrorist side, and OK, careless and clueless can be just as dangerous as those individuals that intended and planned something versus someone just popping up trying to make a YouTube video and actually hit an airplane or violate airspace.

Mr. SWALWELL. Thank you for your service, Sergeant. To the men and women that you serve with, I'll say what we say in our law enforcement family: Be safe. Thank you.

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

I have two more documents that I'm introducing into the record: "Drones in the Wrong Hands: How Criminals Use UAVs to Threaten Prisons and Jails," and another one titled, "New State Drone Law Sets Strict Operational Boundaries."

Without objection, so ordered. I now recognize the gentleman from North Carolina, Mr. Knott.

Mr. KNOTT. Thank you, Mr. Chair. To the witnesses, thank you for being here.

I'll piggyback on one of those submissions. When I was working in law enforcement, the problem had already arrived in many respects. We would send some of the most dangerous people in the country away to jail for sometimes 20–40 years, but there would be no interruption in the criminal enterprises that these folks led, in large part, because of devices and capabilities that made it into the Bureau of Prisons because of the drones. It seemed like just a lumbering bureaucracy and inefficiency that it could not keep up with the technology.

I am curious. Mr. Feddersen, you mentioned that the United States seems to be overwhelmed at this particular juncture. Is the posture of being overwhelmed—is that from just a volume standpoint of all the drones that are in circulation? Is it a technology standpoint, or is it just the layers of bureaucracy that prohibit effective deterrence?

Mr. FEDDERSEN. Thank you for the question. It is a policy, legislative, and bureaucracy issue. Technology is out there today from many companies that have been tested by the FAA, tested by TSA, deemed safe to use at airports, but the confusion over detection, track, and identify has hesitancy across the land, and the fact that the mitigation authorities haven't been expanded in a quick enough manner is—

Mr. KNOTT. What makes sense to remedy this? Because a drone is not an airplane. The fact that they are being regulated as such, in many respects, does not make much sense in terms of placing the same value on a drone as it does an airplane. Should we have a facility-specific code for unmanned aircraft?

Mr. FEDDERSEN. I don't think so, sir. I disagree that labeling it an aircraft hinders anything. It actually gives both operators and those that are working around the drones more protection and coverage into what they're doing. It gives better regulatory understanding of what these drones can and cannot do when they're flying because, honestly, as it has been said before there are drones that are as small as a coffee cup but some that are as big as a car.

Mr. KNOTT. Yes, yes.

Mr. FEDDERSEN. You would have to be able to safely manage that, and aircraft is the right designation for that.

Mr. KNOTT. In terms of fixing the issues that we see, though, how can we fix the bureaucracy and I would say the ineffective legislative posture we have with drones?

Mr. FEDDERSEN. Yes, sir, I'm going to have to point the finger back to all of you on the panel.

Mr. KNOTT. Well, you're the expert. I'm just asking.

Mr. FEDDERSEN. No, because that's exactly what it is. We had a five-year pilot program for a very small sect of Federal law enforce-

ment that started in 2018. We're now in the eighth year of that five-year program. No authorities have been expanded. We have seen that that technology can be used safely and without issue. We've had those departments and agencies ask for an expansion of authorities to get them some relief off their responsibility.

Honestly, especially from being a former State trooper, to say that an FBI agent is smarter and more apt at using this equipment than a State trooper or local law enforcement isn't the right way. The delay is simply understanding the technology and giving trust back to the process and the system.

Mr. KNOTT. What does the technology do specifically?

Mr. FEDDERSEN. It gives you the basic remote—for remote ID information, it tells you where the drone is, what the drone's serial number is, where it's flying, which way it's heading, and where the pilot is in real time. That information can be used for a ground interdiction without even having to worry about the airspace, to talk to the pilot, and have him bring it down.

There are technologies like ours, which is cyber takeover, which takes control of the drone and lands it safely where it needs to be, which then allows for the officer to either give it back to the child and parent with a warning undamaged, no collateral damage, or go ahead and submit for a search warrant to get the information out of the drone.

Mr. KNOTT. Do you think there is a space in the legal construct to have emergency authorization to remove a drone, whether it's shooting it down, taking control of it, or some other means?

Mr. FEDDERSEN. No, sir. These drones are flying at 30–60 miles per hour. The decision cycle for law enforcement or a security individual is literally seconds and minutes. It's not weeks or hours. If it is to be that type of system, then I think it has to be preemptively done to say that a search warrant is going to cover a large area for a large period of time.

Mr. KNOTT. The emphasis of my question is—let's say a drone is flying over an airport, or over a Bureau of Prisons facility. Should there not be the authorization to remove that drone immediately?

Mr. FEDDERSEN. Yes, absolutely.

Mr. KNOTT. Do we lack that currently? Is that correct?

Mr. FEDDERSEN. We do.

Mr. KNOTT. OK. The technology is there to remove that drone?

Mr. FEDDERSEN. The technology is available to remove the drone and remove it safely, and the technology has been tested by the FAA and TSA. A prime example, though, is Federal Air Marshals—

Mr. KNOTT. Yes.

Mr. FEDDERSEN. —who are using the Chinese equipment at our major airports to assess what the situation is, but they don't have authority to use other equipment or use mitigation.

Mr. KNOTT. Mr. Chair, I have more room, but that's—I'll yield back the—

Mr. BIGGS. Thank you. The gentleman's time has expired.

Mr. KNOTT. Yes.

Mr. BIGGS. I now recognize—thank you. We've got lots of questions, don't we?

Mr. KNOTT. Yes.

Mr. BIGGS. The gentleman from California, Mr. Kiley, is recognized for five minutes.

Mr. KILEY. Thanks, Mr. Chair.

Clearly, the problems being discussed at this hearing are extremely serious when it comes to the malicious and unauthorized uses of drones. Of course, there are a lot of good and authorized uses of drones as well for agriculture, for hobbyists, for security, and so forth, and increasingly, actually, for delivery. If you look at companies like Walmart and Amazon, they have actually been expanding their use of drones to make almost instantaneous or very quick deliveries at least of smaller parallels at this point, and that many believe this will become quite widespread in the coming years.

This sort of problem of the unauthorized uses of drones threatens the ability to have that process go smoothly, both from the perspective of having the regulatory process—or framework, more correctly—and in terms of public perception and support for these sorts of things.

Maybe I'll ask Dr. Wallace, and if any of the other panelists want to add to this, how do we sort of address the malicious uses of drones in a way that does not threaten the productive and valuable uses of them?

Dr. WALLACE. It's an excellent question. The initial challenge is there is a misperception that it's easy to identify the misuse of a drone, at least initially. If you're looking at a radar screen, for example, you're going to see a dot and an altitude. That doesn't really give you the ability to immediately distinguish that someone is doing something improperly.

Typically, we leverage information contextually with other kinds of information to try to make some assertions about what is actually happening. Is the drone operating above the altitude that the FAA would permit? Are they operating at an unusual time? Are they operating near a facility that would be questionable? You never really know definitively if this drone is a threat or not. You only have indications.

Mr. KILEY. Thank you. Did any of the other panelists want to weigh in?

Mr. FEDDERSEN. Yes. That the question is a very good question, but it comes back into the fact that when we look at our Nation's airspace, we look at it through two lenses: Safety and security. Air Domain Awareness, which would allow you to see all the drones, is an essential part of the safety aspect of things. It's akin to telling police officers they can't look at certain vehicles that are flying around—or driving around in areas that are off-limits and not being able to react to it. It's the same—you either drive the car legally or you drive the car illegally. It's the same with a drone.

Sgt. DOOLEY. When we do large-scale events, we do have to do a lot of deconfliction. To your point, like, how do you know which one is good and which one is bad? We have briefings prior to large-scale events of our public safety professionals—Amazon, Walmart, if they're doing deliveries in those areas, and make sure that we understand that those are already authorized and we can get a list because, again, it's all about communication and reaching out. We

reach out to our FAA partners and say who has been authorized to fly in this area, because we're going to be their eyes and ears.

If we do have something that is authorized to be there or—to their point, we're not accidentally intercepting or mitigating with our Federal partners. We know that they're supposed to be there, or we already have those clearances ahead of time. Communication is key, and getting out of your silo and talking to the other entities that can do that is key.

Mr. KILEY. Yes. That's very important. If this is going to become more common, deliveries being done in this way, we want folks to have the assurance that these drones are supposed to be there and that they are safe and that they're doing just a routine delivery as opposed to some of the other encounters that people might have in other contexts with drones. I appreciate the work you're doing.

I appreciate the Chair for bringing attention to this issue. I yield back. I would be happy to yield to my colleague, Mr. Knott.

Mr. KNOTT. Thank you, Mr. Kiley.

Sergeant, I noticed that you waved me down when I was talking about the ability to shoot down drones in emergency situations that's not currently within the legal construct. Do you have any insight into how we can best achieve that across, I would say, the sensitive areas, whether they're airports, bases, Bureau of Prisons, what have you?

Sgt. DOOLEY. Well, the ideal means would be nonkinetic. You don't want to, accidentally, a projectile goes up and comes down. There are some scenarios which we've seen overseas where people don't care that you're mitigating, jamming, or GPS denying. They're using fiber-optic and other things to cross these barriers and be very successful, and that may be something that we have to deal with at some point.

We don't want to box our public safety in to just nonkinetic issues, which is basically radio frequency jamming, et cetera. We want to be able to give them a full spectrum of what they feel is necessary to do—or based on their personal experience of what they've encountered, or maybe the intel that they're getting—to be able to handle the situation accordingly. That's my biggest fear, is that we're going to authorize this, but box them in so much that they—

Mr. KNOTT. Yes. They can't respond.

Sgt. DOOLEY. They can't—they are like, I wish I could do something. It would be like me standing on the side of the road with a radar gun and I clock someone going 100 miles an hour, but they didn't give me a car to go chase them down and stop them from that dangerous speed. This is the same thing. We want to have multiple options available to us without being boxed in, but be doing it responsibly with a high level of accountability.

I do think that if we do make a mistake, we should be held accountable. If we mitigate a drone that wasn't supposed to be mitigated, we figure out what went wrong and how we can fix it, but more importantly, document and justify to our Federal partners if we mitigated a drone why we made that decision and what was going on at the time, not just I hit the button, he's not supposed to be there, have a nice day. We have to have some level of that, too.

That will help with the trust part as well in allowing committees like this to approve those type of authorities because we're going to be able to explain when, where, and why we actually did some form of mitigation versus just hitting a button and trusting that everybody is doing what they're supposed to be doing.

Mr. KNOTT. Sergeant, thank you. I yield back.

Mr. BIGGS. Thank you. The gentleman yields back.

This was going to be the last question if I had time, but you touched on this here, and that is has a framework—and I know the answer has a framework been established that clarifies indemnification and liability provisions for law enforcement interacting with drones? Then, my guess is no, other than just general qualified immunity.

Sgt. DOOLEY. From the FAA perspective, there is a law enforcement toolkit that—it gives you things that you're allowed to do if you have to interact with a drone pilot. That you can ask for their registration, you can ask for their trust certificate or part—

Mr. BIGGS. It doesn't deal with—

Sgt. DOOLEY. As far as the mitigation and the detection side, no.

Mr. BIGGS. Right. I guess that's really my question regarding mitigation and detection, that there really is nothing right now—

Sgt. DOOLEY. Other than you can't do it unless you're one of the four Federal entities.

Mr. BIGGS. Right. This leads to the next question.

You kind of addressed it, Mr. Feddersen, and so I may ask all of you.

What is the current framework under the pilot program? What agencies are given authority, what kind of authority are they given, and how do we effectively expand that nationwide?

Mr. FEDDERSEN. Yes, sir. In DHS, there's only a small number of them, small components. There're components out there like his and ICE, the FAMs, and TSA that don't have any authorities that probably should. There on the DOJ side, U.S. Marshals, BOP, you've got DEA and FBI. All Federal components that have authorities are using our system because of the methodology that it has.

The DOD also has it, and you've got—on DOE, falling short of how they're going to go ahead and use things because it's private contractors that particularly take care of power plants and nuclear plants.

The authorities in 124n are fine, because they actually go ahead and do the notwithstanding aspect and waive Title 18 and the Title 49 piece. The issue is training. As long as we have a good solid training program, those authorities in 124n should be broadly spread across the rest of the Federal agency, State, local law enforcement, and critical infrastructure security officers.

Mr. BIGGS. We have—for instance, in immigration law, we provide status for training for departments—sheriffs' departments, et cetera—so they can then enforce certain aspects of immigration law. Is that the kind of thing that might be helpful?

I'm just going to go down—be very quick—and start with Dr. Cahill and go all the way down and finish with Sergeant Dooley.

Dr. CAHILL. That would be very useful, Mr. Chair, in terms of getting it to the people who need it.

Mr. BIGGS. By the way, when I read your statement, I got a kick out of the people that are operating these things while they're drunk. I shouldn't get a kick out of that, but that you reported it kind of made me smile.

Dr. Wallace?

Dr. WALLACE. I would generally agree.

Mr. BIGGS. Mr. Feddersen?

Mr. FEDDERSEN. Yes, sir. Very helpful.

Mr. BIGGS. Sergeant?

Sgt. DOOLEY. Yes. In fact, a lot of our Federal partners have asked, but, unfortunately, that's not an authority they can delegate under those programs like a TFO program. That would have to change to allow us to receive those authorities.

Mr. BIGGS. Right. That would be new legislation we would have to pass to get those authorities in place.

Right now, I want to make sure everyone knows. If I understand correctly, if there is a drone, whether it's a malevolent actor or benign, and it's operating in a restricted airspace, you as local law enforcement—you can't do anything effectively to mitigate?

Sgt. DOOLEY. Mitigating, no. That's it.

Mr. BIGGS. You can make a phone call and say, Hey—

Sgt. DOOLEY. Yes. We can go try to find the operator or try to deal with it, but if we're unsuccessful, that person gets away and we have no record of being able to go back and track it down of where it took off from, who was flying, et cetera.

Mr. BIGGS. We've got major events coming up. We've got Olympics. We've got World Cup. I guess the question is, are we prepared? Are we prepared? We'll just go down this way now.

Sergeant Dooley?

Sgt. DOOLEY. No. I would say public safety could significantly fill those gaps within a—I'm not talking about moving fast and breaking things but moving with a purpose and start filling those gaps pretty quickly.

Mr. BIGGS. Mr. Feddersen?

Mr. FEDDERSEN. No, sir. We're not prepared. The crux of the issue is that, to get systems and people trained and in place before the World Cup and the 250th Anniversary, you have to be able to do an evaluation, determine what you want to buy, secure the funding, and then manufacturers have to get the equipment out and on time for the training.

At that point, we are honestly—Christmas is the deadline for us to be able to do that. If we don't put the authorities in place and expand that to State and local law enforcement, then Federal entities are going to have to do the job, but they're going to have to let something else go.

Mr. BIGGS. Yes. Gosh, I'm out of time. Because I wanted to get to the next point, which is—and you kind of touched on it—what is the time lag to get equipment and train enough personnel to actually be effective for some of these big events coming up?

Go ahead. My time is up, but you can answer Dr. Wallace and Dr. Cahill, really quickly.

Dr. WALLACE. I would agree with my colleagues. We're not prepared, and part of that critical need is the ability to detect, track, and identify.

Dr. CAHILL. I agree we're not prepared, and one of the challenges, of course, is some of these events are very, very spread out. The number of people and assets you need is going to be significant.

Mr. BIGGS. Thank you.

Well, it sounds to me like we need to get on our horse and get a piece of legislation passed very quickly, as quickly as we possibly can. Maybe Representative McBath and I can work together on maybe designating that just, I would say, correlative to the immigration authorities that we give.

With that, I thank all of you for coming today. I appreciate your testimony, again, bearing with us as we started late. Thank you very much.

With that, we are adjourned.

[Whereupon, at 4:27 p.m., the Subcommittee was adjourned.]

All materials submitted for the record by Members of the Subcommittee on Crime and Federal Government Surveillance can be found at: *https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118608*.

○