S. HRG. 119–213

DEFENDING AGAINST DRONES: SETTING SAFEGUARDS FOR COUNTER UNMANNED AIRCRAFT SYSTEMS AUTHORITIES

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MAY 20, 2025

Serial No. J–119–18

Printed for the use of the Committee on the Judiciary

www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
61–982 WASHINGTON : 2026

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

LINDSEY O. GRAHAM, South Carolina	RICHARD J. DURBIN, Illinois, *Ranking Member*
JOHN CORNYN, Texas	SHELDON WHITEHOUSE, Rhode Island
MICHAEL S. LEE, Utah	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	CHRISTOPHER A. COONS, Delaware
JOSH HAWLEY, Missouri	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	MAZIE K. HIRONO, Hawaii
JOHN KENNEDY, Louisiana	CORY A. BOOKER, New Jersey
MARSHA BLACKBURN, Tennessee	ALEX PADILLA, California
ERIC SCHMITT, Missouri	PETER WELCH, Vermont
KATIE BOYD BRITT, Alabama	ADAM B. SCHIFF, California
ASHLEY MOODY, Florida	

KOLAN DAVIS, *Chief Counsel and Staff Director*
JOE ZOGBY, *Democratic Chief Counsel and Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

DEFENDING AGAINST DRONES: SETTING SAFEGUARDS FOR COUNTER UNMANNED AIRCRAFT SYSTEMS AUTHORITIES

TUESDAY, MAY 20, 2025,

UNITED STATES SENATE,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 10:15 a.m., in Room 226, Dirksen Senate Office Building, Hon. Charles E. Grassley, Chairman of the Committee, presiding.

Present: Senators Grassley [presiding], Cornyn, Lee, Kennedy, Blackburn, Schmitt, Britt, Moody, Durbin, Klobuchar, and Blumenthal.

OPENING STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Chairman GRASSLEY. The meeting will come to order. Normally, we don't start without Senator Durbin being here, but he's busy in another Committee and will come along later. I have his permission to move ahead.

Thank you all for coming. Today's hearing will highlight the challenges faced by State and local law enforcement when they encounter drones that pose threats to their own public safety. In 2018, most of us serving on this Committee, including this Senator and Ranking Member Durbin, voted to grant advanced counter-Unmanned Aircraft Systems authority to the Departments of Justice and Homeland Security for public safety functions. These authorities have been extended temporarily eight times since they were originally signed into law in 2018, which is a testament to their importance.

The counter-drone authorities granted to the Department of Justice and the Department of Homeland Security in 2018 left State and local law enforcement out of this framework, but the threats that local law enforcement faces are very much the same. As the threat of dangerous drone use continues to expand and evolve, Congress must find a way to equip law enforcement with the vital tools, while serving civil liberties. These principles are not incompatible.

Notably, the drone industry itself has been asking for clear rules and responsibly deployed counter-drone authorities by State and local law enforcement for several years now. Safer skies are better for everyone, including even amateur drone hobbyists.

Over the years, Congress has heard a lot from the Federal Government on this issue, but today we're going to hear from our State law enforcement officials, telling us their part of the story. The law enforcement professionals here today have unique perspectives on some of the most pressing challenges when it comes to criminal use of drones. These include correctional facilities, where organized crime groups bombard prisons with contraband like dangerous weapons, drugs, cell phones, and tools to aid escape. Illegal drone incursions force prisons around the country to lock down at the expense of those who seek rehabilitation, education, and other programming while serving their sentences.

Drones are also a massive threat at our Southern border, where cartels use them to conduct surveillance of U.S. law enforcement, to smuggle dangerous drugs into our communities, and as weapons of war. We can't wait until a creative criminal or terrorist succeeds in mass casualty attacks before Congress acts. An ounce of prevention is worth a pound of cure, and Federal law enforcement can't be everywhere all at once. But expanded law enforcement authorities must come with oversight and accountability. Our witnesses today will tell you in our Committee that they're not afraid of oversight or accountability. They've already taken oaths to defend the Constitution as well as their communities.

I will play a 1-minute video displaying some of the creative and disturbing ways that criminals use drones. As it currently stands, there's very little our State and local law enforcement officials can do about them, and that needs to change. And that's why we are having this hearing. Would you start the television?

[Video is shown.]

[Voice heard off microphone.]

Chairman GRASSLEY. Okay. Now, if Senator Durbin wants to give his opening statement when he gets here, I'll call on him at that time. And he was going to introduce his witness. I'm going to do that for him; is that right?

Voice. Correct.

Chairman GRASSLEY. Yes. Okay. Our first witness is Captain Troy Wilson. Captain Wilson joined the Texas Department of Public Safety in 1993. Captain Wilson is the Texas Ranger Division Unmanned Aircraft System Program Coordinator. Currently, the Texas Department of Public Safety has approximately 402 UAS aircraft and 384 pilots. The Ranger Division that Captain Wilson coordinates has approximately 67 UAS pilots and 108 U.S. aircraft. Captain Wilson is uniquely qualified to discuss the growing drone threat along the border.

Next is Sergeant Robert Dooley. Sergeant Dooley is statewide UAS counter-UAS coordinator with the Florida Highway Patrol. Sergeant Dooley has more than 23 years of service as a Florida State trooper and has developed and led the Florida Highway Patrol's UAS program since its inception. Sergeant Dooley has a broad range of experience that includes working with other partner agencies at the local, State, interstate, and Federal levels, as well as lawmakers, State attorneys, and other community stakeholders.

Finally, we have president Ricky Dixon. Mr. Dixon serves as secretary of Florida's Department of Corrections and is also currently serving as president of the American Correctional Association. Mr.

Dixon began his career in corrections in 1996. Throughout his early career, Dixon served as a correctional officer, colonel of the Florida State Prison, assistant warden, and warden at three separate correctional institutions. In 2021, Mr. Dixon was appointed to be secretary of the Florida Department of Corrections. He is widely recognized as a—correctional subject matter.

Okay. Introduction of minority witnesses. I'd first like to welcome Jennifer Daskal. Ms. Daskal is a partner with the Venable cybersecurity team. She recently served during the Biden administration as deputy homeland security advisor, principal deputy legal advisor to the National Security Council, and acting general counsel for the Department of Homeland Security.

I also welcome Laura Donohue, professor of law, Georgetown University Law Center, and faculty director of Georgetown Center on National Security and the Law. She is a recognized expert in national security and privacy, technology, and constitutional law as an expert on drones.

Now I would like to do what we customarily do: swear the team. So, would you please rise? And I'd like to administer this oath.

[Witnesses are sworn in.]

Chairman GRASSLEY. I've seen a positive response from all of you. Thank you very much. Now we'll go my left to my right, so we'll start with Mr. Wilson. Captain Wilson.

STATEMENT OF TROY E. WILSON, DIVISION PROGRAM COORDINATOR FOR UNMANNED AERIAL VEHICLES, TEXAS RANGERS, TEXAS

Mr. WILSON. Good morning. Chairman Grassley, Ranking Member Durbin, thank you for inviting me to testify before you today. As you know, my name is Troy Wilson, and I'm a staff captain with the Texas Rangers, with the Department of Public Safety. My responsibilities also include overseeing drone operations within the Texas Ranger Division.

The Texas Ranger Division has been operating UAS on the Texas-Mexico border since 2019. Currently, each week we are sending four special operations group ground teams to the border. Each team is supported by a two-man UAS team. We have operated along the border from El Paso to Brownsville, and these teams work very closely with U.S. Border Patrol and their marine operations.

When we started this in 2019, there was very little UAS used by the criminal organizations, but their ground counter-surveillance was substantial. Currently, they still maintain their ground counter-surveillance but have augmented it with UAS surveillance of law enforcement personnel at all levels. In the past, we have had attempts by criminal UAS operators trying to crash their drones into our drones. We've had their drones hovering above our helicopters. Our helicopters would be at about 1,100 feet, and the drone would be above that, just watching.

We have seen it used to surveil where law enforcement is and is not, on the border. And most recently, about a month ago, one of our drones was mitigated by a cartel across in Laredo, Nuevo Laredo. Transnational criminal organizations use unmanned aircraft along the Texas-Mexico border; it presents a significant evolv-

ing threat. These organizations are increasingly leveraging UAS technology for intelligence-gathering purposes, which enables them to exploit border security operations.

Over the past 12 months, from April 2024 to April 2025, Texas DPS' own sensors have identified 1,216 UAS border incursions. We know this is a fraction of the actual number of incidents, but alarmingly, nearly half of these range in altitude between 600 and 1,800 feet above ground level—the typical altitude range for where our helicopters and border patrol helicopters operate.

The increasing presence of UAS operations in the same airspace as manned aviation introduces an alarming possibility of collisions, endangering the citizens of the State of Texas and law enforcement personnel and equipment. Such incidents critically impair border security operations and endanger lives, underscoring the urgent need for enhanced detection and mitigation systems. The interference with legitimate border security operations, UAS operations by these unauthorized drones undermines critical efforts to maintain control and effectively monitor the region.

Taken together, these threats underscore the urgent need for Congress to grant authority to State and local law enforcement agencies to operate robust detection and mitigation strategies to counter the threat of drones and ensure the safety and security of the border regions. The existing 12 sensors owned by the Texas DPS are limited in scope and only detect DJI drones. This means they only—they make up about 80 percent of the market, and the 12 sensors cover just 14 percent of the 1,200-mile stretch of the Texas-Mexico border.

This illustrates the urgent need to expand sensor coverage both in terms of geography and the variety that UAS can be detected. Addressing these threats requires a comprehensive, layered approach. Detection technologies must be integrated to identify potential UAS threats promptly and accurately, while any mitigation strategies must be implemented with precision to minimize collateral damage. Surgical mitigation techniques are essential to neutralize threats effectively without compromising public safety or causing unintended disruptions.

Above all, we all understand that any counter-UAS detection and mitigation policy or practice must abide by any applicable State or Federal laws and align with the First and Fourth Amendments. Despite significant efforts at the State level, Texas DPS and other law enforcement agencies face constraints imposed by the Federal Government that limit the scope of action needed to address the growing UAS threat. State and local and tribal territory law enforcement agencies need the ability to detect and mitigate criminal UAS along the border and near or over correctional facilities, prisons.

On behalf of the Texas Department of Public Safety, we urge Congress to take action to address this issue. Thank you.

[The prepared statement of Mr. Wilson appears as a submission for the record.]

Chairman GRASSLEY. Thank you. Ms. Daskal.

STATEMENT OF JENNIFER DASKAL,
PARTNER, VENABLE LLP, WASHINGTON, DC

Ms. DASKAL. Chairman Grassley, Ranking Member Durbin, and distinguished Members of the Committee, thank you for inviting me to testify today on an issue of critical importance: the safety and security of Americans from the potential misuse of drones. I will start with a standard disclaimer. I am a partner at Venable LLC and former deputy Homeland Security advisor, but I am testifying solely in my personal capacity, not on behalf of Venable, not on behalf of its clients, and not on behalf of the former administration.

I will also start with the bottom line. Drones serve key public safety, recreational, and commercial functions, and it is absolutely essential that we do everything possible to support the domestic drone industry, including their ability to test and innovate. But as we've already heard, drones also can be weaponized by malicious actors and used carelessly in ways that interfere with lawfully present aircraft and put Americans at risk. We need congressional action to protect Americans from the potential misuse of drones. The bipartisan legislation introduced by Senators Gary Peters and Ron Johnson, included most recently as an amendment to the National Defense Authorization Act of 2025, is, in my view, the place to start.

Drone safety issues rose to prominence during the last 2 months of 2024, when there were numerous reports of drones flying over New Jersey. At the time, I was a deputy Homeland Security advisor. FBI, Department of Homeland Security, Department of Defense, and FAA officials surged resources in attempt to determine what was happening and support local officials, subject to the limits of current authorities. They did not find any evidence of malicious activity, foreign involvement, or criminal action. Instead, it turns out that many of the reported drone sightings were aircraft and helicopters. Others were lawfully present drones.

In early January 2025, the Trump administration reached a similar conclusion. As the President conveyed through his press secretary, "The drones that were flying over New Jersey in large numbers were authorized. This was not the enemy." But at the time, the fear was palpable, and it was justified. The risk of drones being weaponized by malicious actors is real, and the Federal Government lacks sufficient authority and resources to address these threats.

Just last week, on May 13, the Department of Justice arrested a 19-year-old for planning to conduct a mass shooting at a Michigan military base on behalf of ISIS. On the day of the arrest, also the planned day of the attack, the 19-year-old had already launched a surveillance drone in support of the attack. One need only glance at the headlines regarding Ukraine and the Middle East to know how easy it is to purchase off-the-shelf drone technologies and equip them with deadly weapons. And even non-malicious uses of drones, including the careless flying of drones into protected airspace, pose significant risk to aviation security.

Currently, just four Federal agencies—the Department of Justice, Department of Homeland Security, Department of Defense, and Department of Energy—have authority to engage in advanced

detection and mitigation measures to protect Americans from these risks. State, local, and tribal and territorial officials do not have authority to do so, to protect their communities from the misuse of drones. They are wholly dependent on limited Federal support.

In April 2022, the prior administration, in recognition of the current vulnerability, submitted to Congress a legislative proposal that would've expanded the authorities and set of actors who could respond to the misuse of drones. The key elements of that proposal are also included in the bipartisan legislation authored by Senator Peters and Senator Johnson and that I urge Congress to support.

The legislation would do three key things. First, it would expand the authority to detect and mitigate threats to airports, critical infrastructure, and public gatherings. Second, it would give State and local law enforcement officials, as well as airport and critical infrastructure owners, authority to engage in advanced detection measures, helping to ensure the early detection of threats.

Third, it would create a limited pilot, subject to oversight and review, that would give trained State and local officials the authority to mitigate the threats that do emerge. This is a critical element of any effort to provide sufficient protection to the American people, given limited federal resources.

The legislation also includes important safety protections and protections for civil rights and civil liberties. We were very lucky that the 2024 reported sightings in New Jersey turned out to be a false alarm, but next time we might not be so lucky, and I urge Congress to act. Thank you. I look forward to the questions.

[The prepared statement of Ms. Daskal appears as a submission for the record.]

Chairman GRASSLEY. Thank you, Ms. Daskal. Now, Mr. Dooley.

STATEMENT OF ROBERT DOOLEY, UAS PROGRAM COORDINATOR, FLORIDA HIGHWAY PATROL, FLORIDA

Mr. DOOLEY. Good morning, everyone. I'm Sergeant Robert Dooley, and I serve as the statewide UAS coordinator for the Florida Highway Patrol. I'm also proud to be here to represent not only the State of Florida and the Florida Highway Patrol, but I also serve in other capacities, as well. I'm an FAA Safety Team member, which is the educational arm of the FAA. We help and assist public safety agencies with UAS and education training. I'm the director of public safety for AUVSI, the Association for Uncrewed Vehicle Systems International, for the Florida chapter. We started the group in Florida through DRONERESPONDERS, the Florida Public Safety Coordination Group—again, coordinating with our public safety professionals, both law enforcement and fire. And I also sit on the aviation committee for the IACP.

Today, we're here to talk about the critical importance of drone detection and mitigation for public safety. As unmanned aircraft systems continue to proliferate across recreational, commercial, and other domains, the ability of public safety agencies to detect and mitigate unauthorized and threatening drones has become a national imperative. This statement outlines the growing threat and landscape associated with drones, discusses the current challenges in detecting and mitigation, and advocates for urgent integration of counter-UAS capabilities within a public safety framework.

The rapid evolution and accessibility of drone technology has transformed industries and revolutionized emergency response and public safety operations; however, with this growth comes an increasing threat of misuse, whether intentional or through negligence. 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 and preserving critical infrastructure and ensuring operational integrity.

Drones present a unique set of challenges to public safety. Criminal exploitation—as we saw in the video, whether they're smuggling drugs, weaponizing, or contraband into correctional facilities and across the border. I've physically been present at the Texas border. We've been serving out there for 2½ years, and I've seen some of the things that the Captain described. Terrorist use—adversarial States and non-State actors who have experimented with drones for surveillance and weaponization, creating low-cost, low-detection threat vectors. In 2018, in Caracas, two drones were weaponized to go after, if memory serves, Maduro. Both were unsuccessful, but again, we can see how easy it was for them to do that.

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, which is what we saw in California with a drone strike on one of those airplanes—or disaster zones can impede emergency response, creating hazardous conditions for both responders and civilians. Most recently, we had a horrific car crash where—we call it Trauma Hawk, which is the helicopter service that comes and transports patients, and they couldn't take off because there was a rogue drone hovering over the helicopter, and it created a huge hazard.

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 the capacity, agencies operate blindly in shared airspace, increasing the risk to both responders and the public. Some of the benefits to these capabilities would be situational awareness, threat identification, incident mitigation, et cetera. The current limitations and legal barriers—despite the urgent need, most State, local, tribal, and territorial public safety agencies lack the legal authority to mitigate drones and often face limitations even detecting them. Only Federal agencies currently possess this broad CUAS authority, leaving a gap in homeland security at the local level.

Additionally, technology access—CUAS systems are costly. They're complex and often limited to military or Federal use. Interagency coordination—the lack of real-time data-sharing and standard operational procedures hinders unified responses when we are working with our Federal partners and our State partners and our local partners. And policy gaps—existing Federal laws, including FAA preemption of airspace regulation, complicate the roles and responsibilities of our SLTT agencies.

Moving forward, we're asking for legislative reform to grant limited, controlled UAS authority by vetted and trained public safety entities under Federal oversight, as proposed in legislation efforts before. Training and standardization—technology deployment—fund and deploy scalable, non-kinetic drone detection systems to local agencies, particularly those responsible for critical infrastructure and mass events, and also encourage public and private collaboration, where we collaborate with industry to figure out what technology would be appropriate to use and craft it toward specific public safety applications and community engagement, which is probably one of the most important ones.

In 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 front lines of both natural and manmade crises, and their lack of CUAS capabilities leaves a critical vulnerability in our national preparedness. The 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.

And that is it. And I await your questions. Thank you.

[The prepared statement of Mr. Dooley appears as a submission for the record.]

Chairman GRASSLEY. Thank you. Professor Donohue.

STATEMENT OF LAURA K. DONOHUE, PROFESSOR OF LAW, GEORGETOWN LAW, WASHINGTON, DC

Professor DONOHUE. Thank you. Chairman Grassley, Ranking Member Durbin, and distinguished Members of the Committee, thank you for inviting me to today's hearing. UAS are part of our daily lives. They're used for agriculture, construction, sports broadcasting, film production, and myriad other peaceful purposes. They act as first responders. They're used for artistic expression. UAS also can be levied by States and non-State actors for nefarious purposes. They carry drugs, guns, bombs, flamethrowers, and CBNRW. They can be outfitted with tracking technologies enhanced by biometric identification. Autonomous swarms present further challenges.

It's important that we have the authorities necessary to meet these threats, but what Congress passes cannot be a blank check. It needs to be carefully drafted to take account of constitutional rights. The law currently raises troubling First, Fourth, Fifth, and Tenth Amendment concerns.

On the First Amendment, courts have long considered video recording to fall within freedom of speech and the press. The right to obtain footage includes the right to record government employees in public space. That ability undergirds one of the primary First Amendment aims, which is to hold government officials accountable.

That right is not absolute, but provisions which impact that right cannot "burden substantially more speech than is necessary to further the Government's legitimate interest." The statute, on its face, violates this test. There are no limits on the Government facilities which are covered. There's no requirement for distance from the facility, the direction of travel, or whether the drone is over private

property. There's no showing that must be made about specific targets. The provisions could be used to prevent media coverage on matters of great importance to the electorate. It has already occurred.

The AG guidelines detailing covered facilities are similarly troubling. To determine whether activities constitute a credible threat, seven possibilities are offered, some of which—such as the reasonable belief that UAS could harm a person or damage property—it's true of all drones. Six of the seven have no nexus to any facility or asset, and any interference in the execution of government activity counts, potentially including lawful protest.

Further, to satisfy the requirement that the facility be connected to an authorized mission, the guidelines include any National Special Security Event, which is defined as a designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity. All of those are core First Amendment protected activities.

The right to petition, moreover, applies to all three branches and promotes continual active political engagement. Courts use an experience and logic test to determine whether there's a qualified right of public access to public facilities. The law, however, allows the Government to forbid access to all Federal facilities and Federally owned land without regard to its historical use.

On the Fourth and Fifth Amendments, one of the most glaring concerns in the statutory language is that it essentially operates as a general warrant, which is forbidden under the Fourth Amendment. A general warrant is a document issued by an official, not based on any evidence of wrongdoing. It lacks particularity in the person or place to be searched or the papers or records to be seized. Unsupported by oath, it's used to find evidence of criminal activity. At the founding, such documents violated the reason of the common law and were thus unreasonable.

The current law gives the Government the authority to access all communications between the operator and the drone, to seize control of all UAS systems, and to search devices to find evidence of illegal activity. There's no oath, no third party, no probable cause. The act is a general warrant.

RF drone detection systems share similarities here with geofence warrants in criminal law, which compel companies to provide location data from users' devices. They also lack particularity, but unlike the drone provisions, geofence warrants involve third-party magistrates, a demonstration of probable cause, and an oath. Even so, circuits are split as to whether they constitute general warrants. For the Fifth Circuit, they do. 124n suffers from the same constitutional defect.

Finally, on States' rights, control of real property—including the airspace above land, outside of Federally owned property—falls in the purview of States. It's reserved to them through the Tenth Amendment. There's nothing in the Federal provisions which acknowledges State control over adjacent airspace, much less State rights to operate their own UAS over public property. These deficiencies can be addressed to assure the Government has the power to protect against UAS, while protecting constitutional rights.

First, Congress could require a probable cause warrant to target specific drones under the protective measures, subject to exigency exceptions as well as the border exception. Second, Congress should institute substantive First Amendment protections. And, third, Congress should respect State rights by ensuring that States have the lead for drones under 400 feet and exempting State drones from Federal targeting. Thank you.

[The prepared statement of Professor Donohue appears as a submission for the record.]

Chairman GRASSLEY. Thank you, Professor. Now, Mr. Dixon.

STATEMENT OF RICKY D. DIXON, PRESIDENT, AMERICAN CORRECTIONAL ASSOCIATION, FLORIDA

Mr. DIXON. First of all, Chairman Grassley and members, thank you so much for the opportunity to speak on this important issue today. Again, my name is Ricky Dixon. I'm the secretary of the Florida Department of Corrections, and I currently serve as the president of the American Correctional Association. I'm here today representing several hundred thousand correctional professionals across this Nation who work tirelessly to maintain order, security, and provide rehabilitation within our facilities. I've spent nearly 3 decades in this profession, starting as a correctional officer and working through the ranks to lead one of the largest prison systems in the United States.

I tell you that to say that I know firsthand the urgent threats facing our staff, the inmates we house, and the public we serve. Now, I'm here today to sound the alarm and make you aware of a growing crisis within our profession, one that calls for immediate action. The criminal use of unmanned aircraft systems, or drones, is escalating, and we do not have the tools or the legal authority to stop them.

These drones are no longer just a nuisance. They're sophisticated weapons for organized crime, smuggling fentanyl, heroin, razor blades, weapons, and contraband cell phones into our facilities with precision. Each time a drone enters our airspace, we're forced to lock down, halting education, job training, drug treatment, and mental health programs—programs that reduce recidivism and prepare individuals for successful reintegration into society; programs you've appropriately supported and allocated funding for. The consequences—they're deadly.

Drone-delivered narcotics have led to numerous overdose deaths inside our prisons throughout this Nation and contribute significantly to violence against other inmates and our staff. But make no mistake. This crisis is not just a local issue. It does not end at our facility gates. Contraband cell phones, smuggled in by drones, are powerful criminal tools. From behind bars, inmates are orchestrating drug trafficking, intimidating witnesses, and directing violent crimes in our communities.

Families are being extorted, forced to send money to protect loved ones from harm inside the prison walls. Inmates are being brutally assaulted to serve as examples of what can happen when families don't comply. American prisons are turning into command centers for drug cartels and gang leaders, driving crime well beyond our fences.

It's only a matter of time before a firearm or firearms are dropped in by drones, with timing synchronized with cell phones so that a specific inmate or group of inmates are in a position to receive them, in an effort to take over a facility. All of this happens at a time when staffing shortages are already pushing our workforce to its limits. Officers are working mandatory overtime, just to keep operations running. Adding drone-related lockdowns, heightened security demands, and emergency searches makes their jobs unsustainable. Yet, despite the severity of this issue, correctional agencies remain legally prohibited from taking action.

Only four Federal agencies have the authority to counteract drone threats. Meanwhile, State and local correctional facilities, among the most frequently targeted, remain defenseless. Waiting for Federal intervention is putting lives at risk. We appreciate legislative proposals for pilot programs to test counter-drone solutions, but let's be clear. Pilot programs alone will not solve this national crisis.

The issue requires a comprehensive, scalable, and well regulated legal framework—one that grants correctional and law enforcement agencies the authority for advanced detection and mitigation, backed by funding, training, and oversight. Every authorized drone that enters correctional airspace undermines public safety. Every contraband cell phone delivered by drone strengthens criminal enterprises, and every lockdown caused by drone activity hinders rehabilitation and destabilizes institutions.

We urge you to act. Give us the tools, the authority, and support we need to support this growing threat before it spirals further out of control—to stop this growing threat; sorry. The safety of our correctional facilities, our workforce, and our communities depend on it. Without this authority, we allow modern technology to become a weapon that undermines justice, facilitates contraband trafficking, and jeopardizes lives: threats the framers never intended the First, Fourth, Fifth, or Tenth Amendment to shield.

I'll leave you with this. This issue will be addressed eventually; there's no doubt. The only question is whether we act now with foresight or wait for disaster and attempt to recover after the fact. Thank you, and I stand ready to take any questions.

[The prepared statement of Mr. Dixon appears as a submission for the record.]

Chairman GRASSLEY [off mic]. Finance Committee, so I hope somebody on my side of the aisle will take over while I'm gone. Captain Wilson, in your testimony you mentioned an incident in which Texas State law enforcement drone was actually mitigated by Mexican cartel members. Can you please elaborate on the challenge that you face from cartel drones and speak to the safety of the risk to your department faces by not being able to employ the same technology that cartels have started to use against U.S. law enforcement?

Mr. WILSON. Yes, sir, Mr. Chairman. The——

Chairman GRASSLEY. Push your button.

Mr. WILSON. That would help, wouldn't it?

Chairman GRASSLEY. Yes.

Mr. WILSON. Mr. Chairman, in 2019 they started the ground surveillance. They would follow us for 1½, 2 hours, back to our hotels

from where we were working on the border. People are sitting in a tree or sitting on a fence line. All they're there for is to scout for us, for law enforcement: for Federal, State, local law enforcement. UAS has increased significantly since then, to now where they're—like I mentioned earlier, they're trying to crash drones into our drones; they're trying to—they're hovering over our helicopters at 1,500, 1,600 feet, clearly above 400 feet, and presenting a clear danger to any manned aviation in that area.

In the last month, we were mitigated by the cartels. We were in conversation or in communication with U.S. Border Patrol. They had asked us to see if we could—they had a detection over in Mexico, and we're asked to see if we could find the pilot for that drone. After a little bit of time, we were able to locate that pilot and follow him.

There was communication with Mexico to try to get the Government there to respond, and as they were responding and before they got into the area, the criminal drone came down and departed the area. We continued to stay with the pilot and his co-pilot, if you will, to—eventually, our drone lost connection and was mitigated by the cartel, as we found out later, and crashed about 1,000 feet away from where the mitigation took place.

Chairman GRASSLEY. Thank you for that. Sergeant Dooley, you and your office provide support for Federal law enforcement at mass gatherings and during protective operations. I'd like to have you elaborate on your role providing this support and explain how enhanced counter-UAS authorities would better enable you to support Federal partners.

Mr. DOOLEY. Yes. So, that's a huge request we get. A lot of our Federal and State partners know that we have the ability to do that. In most cases, our Federal partners are—their equipment is much more sophisticated than what we're allowed to use, but it is of—still—use. That's the number one question I get when they ask for our help, when we're using our equipment to help them in their detection—is, can we mitigate? And, of course, my response is, no, we can't do that.

They have a desperate need, I think, for a force multiplier and a support from the State, when we especially have our Federal partners who rotate in and out from certain details and come to Florida. They're not the same people, normally, over and over again, so when they come down and they are not terribly familiar, and we educate them on what our capabilities are and how we're supporting them already, again, over and over again: Can you help us mitigate?

No, we cannot. Our technology is passive. We use radars, cameras, remote ID, et cetera. We don't get into hacking and RF and all those things. But again, it still helps; it's just not on the level that they can perform those same duties. But it is a huge request that we get for those capabilities.

And on top of that, I will get phone calls from our Federal partners, as well, when they do have a request—because most of the requests that our Federal partners get can't be fulfilled. They don't have enough resources and equipment, et cetera, to cover all the requests. And they'll call me. And again, I can't perform some of the same duties that they can, so it's—and in some cases it is of

no use, because what they need specifically is the mitigation or the ability to detect on a higher level than what we're able to provide.

Chairman GRASSLEY. Okay. Mr. Dixon, in your testimony you mentioned the dangers that drone-delivered contraband like weapons and cell phones present to prisons. Elaborate on the threat of contraband cell phones to prison security.

Mr. DIXON. Sure, Mr. Chair. So, cell phones and drones, combined, are a few of the most critical security threats we have right now. The irony in this is drones deliver cell phones, and the very cell phones that are delivered are what is used to coordinate additional drone deliveries. Everything bad that happens in a prison usually starts with a conversation. So, if we intercept or prevent the cell phones that are delivered by drones, we reduce a significant amount of the violence.

As I mentioned in my testimony, cell phones are used to extort families, to maintain criminal networks on the street. As I mentioned, prisons in some cases are command centers for drug cartels, because they continue their criminal enterprises. If we eliminate cell phones and drive the communication back to our State systems, we have sophisticated tools to monitor those systems, whether it be on our tablets or our institutional phone systems, but when they, you know, circumvent that through cell phones that drones deliver, it's one of the major issues we have to combat.

Chairman GRASSLEY. Thank you. Senator Durbin.

OPENING STATEMENT OF HON. RICHARD J. DURBIN, A U.S. SENATOR FROM THE STATE OF ILLINOIS

Senator DURBIN. Thanks, Mr. Chairman. Let me apologize for coming in late. I had another hearing, in Appropriations with Secretary Kennedy, and I'm sorry I missed the opening. Special thanks to Ms. Daskal and Professor Donohue, our witnesses that I was not here to introduce. Thanks, Senator Grassley, for doing that.

So, I'm sure most of us were watching the Cubs-Sox series in Wrigley Field this weekend. And I was struck by the fact that they were doting on the capacity they had with the drone to show images of Wrigley Field from angles and perspectives never known before. It was beautiful, and the Cubs won, so it was a good day all around. But it raised a question in my mind that I wanted to pose to several members of the panel here.

If I were sitting in Wrigley Field with a friend or son or granddaughter, and I saw a drone overhead, I would want to be sure that it was a safe and friendly drone. I don't know that, when I'm sitting there. Somebody has to find out or at least ask the question. With over a million drones in our country today—and drones possibly hovering over fields of sports and other things—it raises the question of who's going to monitor that activity to make sure these are safe vehicles, air vehicles, that don't endanger anyone.

At the same time, those drones could be gathering information, not so much at a ball field, but maybe you're going to have a wedding at someone's home. There's a privacy angle there, too. Who's protecting the privacy of the people that they are broadcasting or gathering information on? So, I'd like to ask Professor Donohue, how do you balance this? The drones over Wrigley Field—are they

friendly or not? The gathering of information in my own back yard—is it anybody's business? Who's protecting me?

Ms. DONOHUE. Thank you very much for the question. As a matter of large-scale outdoor events, for instance, most States have regulations and laws in place that prohibit the flight of drones over certain large-scale events. They require that there be agreement—some consent from the property owner or from the venue owner—in order or some sort of contract in place.

In terms of how to balance those rights and the privacy, most States—they actually have carve-outs saying that others cannot fly drones over private property without the consent of the property owner themselves, because owing to this ancient doctrine of ad coelum, property owners own the adjacent airspace over their land. And so they have the right to exclude drones. That——

Senator DURBIN. Let's talk about the practical world. You've got air traffic controllers monitoring commercial aircraft, other aircraft, but in terms of monitoring actual drone activity to the point of knowing whether it's complying with the State law—and if it's not, what to do about it—what's the answer there?

Ms. DONOHUE. Anything below 400 feet is within the State domain; that is adjacent airspace.

Senator DURBIN. How is it enforced?

Ms. DONOHUE. Through State monitoring of this. There are agreements with the FAA. For instance, if you need to have a temporary flight restriction over particular areas, as during, for instance, the Super Bowl, in those cases, the way to balance the civil liberties concerns is to make sure that there are restrictions.

For instance, you don't extend the Super Bowl coverage for a month, and you don't extend it over any land or any drone anywhere in the country, but it has to be a drone that's actually adjacent to that particular site. So, when the Federal Government is involved, if there's the potential for the Federal Government to take down a drone or to interfere in its operation or to conduct a search of the device itself, then there needs to be some nexus to the actual open-air facility or the place that's trying to be protected.

Senator DURBIN. Professor Donohue, if counter-drone authorities are not drafted carefully, could they permit government authorities to intercept data or communications in violation of the Fourth Amendment?

Ms. DONOHUE. Yes.

Senator DURBIN. Thank you for that. Mr. Chairman.

Chairman GRASSLEY. Senator Lee.

Senator LEE. Thank you, Mr. Chairman. Thanks to each of you for being here. Over the last 15 years or so, drones have become increasingly a part of our lives. They've been used not only by the military, by law enforcement, by immigration authorities, but also by businesses, hobbyists, and other kinds of enthusiasts. Yet in some instances, drones can present threats—grave threats, pretty dire threats. Meanwhile, the current regulatory framework creates a problem insofar as it inhibits State and local law enforcement from adequately addressing those same threats that can be uniquely posed by drones.

That's why I introduced a bill called the SHIELD-U Act: Stopping Harmful Incidents to Enforce Lawful Drone Use. And this legislation, once enacted, will help State and local law enforcement by giving them authority, on a limited, constrained basis, that they need in order to protect their citizens and their communities from those who would use drone technology to harm the public.

Sergeant Dooley, let's start with you. Now, you've testified about the limitations imposed by Federal law that effectively prohibit State and local law enforcement—in fact, they expressly prohibit them—from effectively utilizing counter-drone, counter-UAS systems. This bill that I referred to, the SHIELD-U Act, lifts some of those restrictions. How would passing that bill and granting limited counter-UAS capabilities enhance State and local law enforcement and your ability to protect the public?

Mr. DOOLEY. Well, number one, I agree with almost everything that was said earlier—is we do need some significant oversight. We need accountability. We need training. We need all these things. Like, someone like me shouldn't exist, where I had to figure it out on my own because there was no——

Senator LEE. Well, you should exist.

Mr. DOOLEY. Well, but you understand what I'm getting at? There should be some type of oversight, guidance, and training where we could establish that, and then when this was rolled out, it would be controlled. Like, you know, how would you mitigate something? Okay, why would you even set up a system in the first place in a particular location? Justify it. Why are you here? What are you going to do, if you saw a drone in the airspace? Are you just detecting it, that it's there and it's minding its own business, or is it a threat? Why did you do what you did?

But the bill would dramatically increase our ability to keep critical infrastructure, VIPs, other mass—like sporting events—a lot safer and people—like, to the other Senator's point, you know, when you see a drone flying over the Cubs game, is it a friend or foe? And that's what we would like to do: not necessarily interfering—and, again, regulating what exactly is being detected.

Remote ID, for example—it's not great. It's hard to detect at times because every drone broadcasts it slightly differently, but if you were doing standard RF detection or something of that nature, where it's only picking up what type of drone it is and serial number; it's not telling you anything about the operator or the person operating it—nothing personal, right—we still have to go and follow the legal process to get that information—I think it would be of great use and of great help to public safety, if used in the proper way.

Senator LEE. That's a great point. You know, I like the way you phrased it. It reminds me about an analogy Robin Williams once referred to: the unarmed English bobby who, being unarmed, upon seeing the commission of a crime, yells, stop, or I'll yell stop again. But if you can't do more than that, there are going to be problems, and that's something we face with drones.

Captain Wilson, let's go to you next. Now, you've highlighted the need for counter-UAS capabilities at and near the border. If State and local law enforcement capabilities were unleashed in the counter-UAS sphere, how would law enforcement efforts at the bor-

der be improved corresponding to that, or as a result of that, I should say?

Mr. WILSON. It would allow us law enforcement at all levels to work closer together, to have—again, identify those locations that we wish to have a sensor and based on activity or that's going on, and it'd keep us and the community safer, being able——

Senator LEE. It would help?

Mr. WILSON [continuing]. To detect—yes, sir—and detect and then, if necessary, mitigate.

Senator LEE. Secretary Dixon, when drones are detected overhead a prison, a correctional facility, what are the security protocols that you go through, once you see it?

Mr. DIXON. Thank you, Senator, for that question. It's quite extensive. We lock the compound down. That could be for hours, days, weeks in some cases, depending on the payload that—the portion of the payload we discovered, if at all. Significant consequences occur, between gangs and different members and different inmates in the institution, if the payload doesn't make it to its intended target. So, it's a dangerous situation. It, as I mentioned earlier——

Senator LEE. So, there's no way that that doesn't compromise your ability to operate correctional facilities in a manner that is effective and safe.

Mr. DIXON. It absolutely does, in addition to—as I mentioned earlier—stop all the rehabilitative programming, the mental health programming. All those functions that we're supposed to carry out, we put on pause at a time we're already in a difficult staffing situation.

I do want to—in appreciation for Senator Durbin's comment earlier, as well, I do think there's a differentiation to be made between our environment in the prison setting versus the citizenry. You know, when it comes to the Fourth Amendment, there's no reasonable expectation of privacy for those people we house there, and so we're simply asking for that—when drones enter our airspace, to be able to deal with them and mitigate the threat at that point.

Senator LEE. Thank you. Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Klobuchar.

Senator KLOBUCHAR. Thank you very much. Thank you all. This has been really interesting testimony. I think, what, there's over a million drones registered with the FAA that can be used for some really good stuff. Farmers in Minnesota are using them for farm management; civil engineers for surveying. I especially see this in rural areas. When we have everything from train wrecks on, they're incredibly helpful.

We also know the risks. You just brought up this, Mr. Dixon, at the correctional institutes, and I hadn't thought through all that. Thank you. We know that there's privacy concerns which—and our liberties, which Senator Durbin, I know, discussed.

I just want to start with something that's on my mind a lot, Ms. Daskal, and that is commercial aviation. As you noted in your written testimony, drones accounted for nearly two-thirds of near-misses with commercial passenger planes, which is kind of an extraordinary number. You also noted that airports lack critical authority to protect against drone incursions. We saw what happened

in LA with the firefighting plane at a time of just critical danger. What authority should Congress provide airports and other critical infrastructure operatives to ensure they're able to protect the public?

Ms. DASKAL. Thank you, Senator. I share the concerns, particularly the concerns around airports and critical infrastructure. And as I said in my testimony, I think that the legislation, the bipartisan legislation that was introduced by Senator Peters and Senator Johnson, is——

Senator KLOBUCHAR. Yes, I think——

Ms. DASKAL [continuing]. A really good place——

Senator KLOBUCHAR. Yes.

Ms. DASKAL [continuing]. To start, and it does a couple of things. First, it gives airport owners and critical infrastructure owners new authority to engage in advanced detection measures which they don't currently have, to be able to identify the threats that do arise. That is important. It's also subject to training requirements, to privacy compliance requirements, to the use of technologies that are tested and approved. And, secondly, the other piece of this that I also think is critical is ensuring that State and local authorities have the ability to mitigate, as appropriate, subject to oversight and review.

Senator KLOBUCHAR. Thank you. Yes, I think I'm a co-sponsor of that bill, and I hope we can move that. News organizations—you know how we have to protect their right to be able to take photos and the like, of disasters, so the public knows that. Could you talk about balancing the uses that news organizations have for drones, so that they don't interfere with public safety? Quickly.

Ms. DASKAL. Yes, absolutely. So, as you know, Senator, the FAA has the authority to put in place temporary flight restrictions for a range of reasons, including safety and security reasons. There is also a process by which media organizations can seek waivers in the event that there are temporary flight restrictions, in order to engage in First Amendment-protected activity and to ensure that the public is made aware of critical information. And those waivers—that process needs to continue.

Senator KLOBUCHAR. Okay. Thank you. Sergeant Dooley, in your testimony, your written testimony, you suggested granting State and local law enforcement limited counter-UAS authorities, subject to standardized training and certification. There are examples of this across law enforcement. For example, all bomb technicians across the country are trained at the FBI's Hazardous Device School. How would you envision this standardized training?

Mr. DOOLEY. Number one, it would have to come from, I think, one of our Federal partners that's already been authorized to do this and has been doing it. They would have the most experience. Number two, I don't think that everybody necessarily would need this right off the bat. I think there should be some level of credentialing as to different levels of detection and mitigation, as well. You may have, like, a multitiered approach of someone that just can simply detect and do nothing about it because of whatever reason, and then you go down the list, and then you may have more critical infrastructure or maybe a higher profile target area that may need those additional permissions.

I think that you should have, like—for example, like, just to be a drone pilot, I have to get a Part 107 airman's certificate, right? I have to register my drone. There's a processing place. When I wanted to drive a car, I had to go take a driving test. Like, there's tests for everything. I wanted to be a trooper; had to go——

Senator KLOBUCHAR. I got it.

Mr. DOOLEY. Yes. So, this is no different. I think we could figure it out to where——

Senator KLOBUCHAR. Okay.

Mr. DOOLEY [continuing]. There would be different levels.

Senator KLOBUCHAR. Got it.

Mr. DOOLEY. I think one of the four should definitely be the starting point——

Senator KLOBUCHAR. Okay. My——

Mr. DOOLEY [continuing]. Of the four Federal agencies.

Senator KLOBUCHAR. Thank you. My last question: Mr. Dixon, you talked about things being smuggled in through drones into prisons. You also noted that correctional facilities are legally prohibited from employing counter-UAS technology. Could you talk about the threat to correctional officers and inmates at a facility?

Mr. DIXON. Thank you for the question. Absolutely. Anytime drugs are introduced to the compound and the kind of contraband that comes in—it increases the threat, in terms of—I've seen a, you know, 98 percent increase in outside medical trips, for security, in the last several years, much of that related to the contraband drones bring in. It's one of the most dangerous things we do—is take inmates outside of our fence to local hospitals. The violence that's associated with drugs coming in, the contraband coming in has increased exponentially since this became a problem.

Senator KLOBUCHAR. And, last, just—when the drones breach the perimeter, it's obviously a major threat, but what type of counter-UAS authorities do correctional facilities need? And make it quick, because I've gone over my time.

Mr. DIXON. And we're not resistant at all to oversight and training, but we need the ability to mitigate that threat to a greater extent than we do now, to intercept those drones coming over our facility.

Senator KLOBUCHAR. Thank you.

Chairman GRASSLEY. Senator Britt.

Senator BRITT. Thank you, Mr. Chairman. Thank you for holding this hearing today on this important topic. I hear this from people all across Alabama: The lack of drone mitigation authority for State and local law enforcement has become a critical issue. We see it specifically when we're looking at large public gatherings, which includes large sporting events, which my State takes great pride in. And we want to make sure that public safety comes first.

Even when it comes to Federal installations in Alabama, it's often State and local law enforcement and personnel who are the closest and most capable of actually responding. We see this, too: Our Alabama Law Enforcement Agency, who is headed by Secretary Hal Taylor, who does a tremendous job—they assist Federal partners and are likely the first ones to be able to respond and to do it in a meaningfully and efficient way. But without proper au-

thority, they can't act with the speed and coordination that they need, that matters most in a time of a crisis.

So, I'm going to address this question to Captain Wilson and Sergeant Dooley, to start with. Is there a legislative solution that is as simple as just extending existing mitigation authorities to State and local law enforcement, that would actually help in these situations? Or is there other gaps in the law that needs to be considered? And what should our top priorities be when considering a legislative solution to actually address this issue?

Mr. DOOLEY. We looked at it extensively, especially when we started working with our Federal partners. Those permissions were granted by Congress, right?

Senator BRITT. Mm-hmm.

Mr. DOOLEY. So, they can't be delegated. Like, for example, some TFO programs—temporary Federal officer programs, where the U.S. Marshals will deputize local law enforcement with certain abilities to do U.S. Marshals things—we looked into that, and again, we feel that the authority couldn't be delegated. Like, that would've been the simplest approach: Deputize me as whatever——

Senator BRITT. Right.

Mr. WILSON [continuing]. And under your supervision or guidance, we would move forward and do this. But we don't think that's correct. So, I don't know what we would do as a simple solution, other than—we're in this room here trying to figure it out. But we've tried to look down some of those legal avenues of doing it correctly, but we—that was what we came up with, and they can't delegate those authorities if they were to bless us as a TFO.

Mr. WILSON. Yes, and like Sergeant Dooley said earlier, that it has to be—there has to be training, and there has to be some accountability. There has to be transparency for all the agencies that start, and you're going to have to start somewhere with some credentialing of some law enforcement agencies at the appropriate level, to work.

Senator BRITT. So, are those things that we could be doing right now? What are things that we could be doing right now to make sure that we're preparing for that, that we're taking proactive steps to be able to allow State and local law enforcement to have this capacity or this ability in the future?

Mr. DOOLEY. So, I think, like, right now you should probably establish, like, who would run this, from——

Senator BRITT. Okay.

Mr. DIXON [continuing]. A Federal level. That would—once we get started with that, then we start figuring out how we should roll this out, who should be a part of the initial rollout, and what type of equipment we should be using—and, more importantly, some type of process in place of standardizing how this is used: a reporting process in place, et cetera, to where if I do deploy something and we do detect and we do mitigate or whatever it is, that there is proper—like we talked about, multiple times, of accountability.

So, if I'm right, everything's fine; I submit a report. If I did something wrong, we can identify it and either correct it or discipline or whatever the case is. There has to be right or wrong. We have to have transparency to do that. But I think we should identify a

Federal entity of some sort that should control this, moving out toward public safety having this——

Senator BRITT. And is the training in place now to be able to make these moves?

Mr. DOOLEY. No, ma'am.

Mr. WILSON. No.

Senator BRITT. So, we would need to be able to invest in that, as well?

Mr. WILSON. Yes.

Mr. DOOLEY. Yes.

Senator BRITT. Okay. I want to turn to you, Secretary Dixon, in my last few minutes. In Alabama, like most other States, we have seen an increase in drones—using to fly contraband into correctional facilities. As you have testified today and spoken with my colleagues about, that presents a real risk not only to inmates but obviously the officers, as well. Based on your experience, can you kind of explain to us some of the unique challenges related to drone mitigation when it comes to a correctional setting and how those should inform us as we're looking at potential legislation?

Mr. DIXON. Thank you, Senator. One of the most significant challenges is that they come in and we don't know they're there. Often they fly—sometimes they fly high. They're fast; they're swift. So, often, the contraband is delivered and we never saw it coming, so we're defenseless. We have limited systems that help detect when they're coming in, but not nearly as advanced as they should be, as the technology is capable to deliver right now if we had the Federal authorities we need.

And I would just like to add, not to be melodramatic, but I would encourage us to act with the same sense of urgency that we would if we were watching on the news right now that multiple automatic weapons were just delivered into one of our compounds by drone, and to gang members, and they escaped or harmed or killed other inmates or staff, because that is a very likely scenario. That's not being an alarmist; it's very likely. And I'm not implying we're not—it's why we're here today, and we're so thankful that we're having this discussion.

Senator BRITT. Thank you so much. Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Moody.

Senator MOODY. Thank you. It's not too often I get to go behind my fellow junior Senator.

Senator BRITT. That's right.

Senator MOODY. Thank you, Mr. Chairman, for holding this hearing and for all of the witnesses for taking time away from your jobs and your families to be here in Washington, especially to my fellow Floridians. Very proud of you. Thank you for being here and representing the great free State of Florida.

I think something that resonated, Mr. Dixon—what you said was, act with a sense of urgency: something that we in Congress don't take to heart a lot around here. As a mother, I certainly do, because I know what we do right now in this Congress will protect or leave vulnerable many Americans and certainly our children.

In Florida, we are home to many military installations. Certainly, we have three combatant commands in our State. The sensitivity of what is taking place within the State of Florida, not only

on military bases—also on our Space Coast. Most of our launches are done from Kennedy Space Center. So, we have a lot of sensitive personnel, information, movements, commands right in the heart of Florida. And I know that, Sergeant Dooley, with FHP, you are coordinating the UAV program there, and you assist when there are incursions in military space and violations and use State assets to help with that. I want to thank you for being an expert and for your attention on that.

One of the things that I have been trying to highlight and have passed legislation to do is to stop visas right now, student visas, particularly, from the Chinese government, because they have laws in place right now that require their citizens to gather intelligence and work with the CCP, and yet we're importing 300,000 a year into the United States. And particularly I want to point out an example. In August 2021, we allowed in to study one of these students, to study at the University of Minnesota, and particularly, thereafter we're told that he was gathering information from military bases.

On January 18 of 2024, the FBI arrested him in San Francisco for operating an unarmed aircraft system in violation of national defense airspace and photographing defense installations. Further investigation found that he had taken photographs and used a drone to photograph the naval base in Norfolk, Virginia. Here on a visa to study at the university. Thankfully, he was finally deported just a couple of weeks ago and sent home. Thankfully, we have an administration that's taking these things seriously now.

But this is a weakness, I believe, in our Espionage Act, in the sense that we outlaw photographing military bases using drones. In fact, in this particular case, they found video on this drone, but they could only charge the photographs. It's a weakness in the evolution of technology that we have failed to update our laws. And so I would ask you, Sergeant, is this something that you believe we need to shore up, to make sure we can criminally charge, when we don't just have foreign agents taking photographs of sensitive military bases and installations but also video?

Mr. DOOLEY. Yes. No, I totally agree. And we also have some pretty robust statutes in Florida that also allow law enforcement or public safety to have at least a little bit more teeth in the bite when we do have some type of these situations: Florida Statute 330.41 and 934.50, which also protect people's rights to privacy with drone operations, et cetera. So, I completely agree that we should figure something out and make it to where these things can't happen.

Senator MOODY. And Mr. Chair——

Professor DONOHUE. Senator, may I possibly add——

Senator MOODY. One moment. I just want to say, Mr. Chairman, today I'm going to introduce the Drone Espionage Act legislation, which would include—it would strengthen the Espionage Act of 1917 and include videography of sensitive national defense sites as a crime; include videography in addition to photographs. This is an issue that doesn't just affect Florida. All of the members here have sensitive military sites in their States.

Many Congressional Members have States where folks have come over here on visas; foreign nationals have been caught

videoing sensitive military sites in this country. And we have to put an end to it. It has to be a crime. And I appreciate the time, and I'm sorry I have run out of time. And I will leave to the Chairman whether or not he wants to permit additional testimony.

Chairman GRASSLEY. Is there any comment from any of you on her last point?

Professor DONOHUE. Yes, please. I just wanted to comment on the last point. I also build drones, and I work in national security issues, so thermal imaging, lasers, like LADAR; the use of other imaging and sensor technologies—it is a gap, in my view, in the Espionage Act, and it is something that needs to be addressed. I also just wanted to add the border exception here, because obviously along the border—case law is very strong in showing that there's an exception to warrant requirements along the border because of national interest, within at least 20 miles of the border if it's contiguous with entering and leaving the United States.

So—and then the third point is the military sites are precisely the kind of sensitive facility that should be subject to these types of provisions, but that's very different from, you know, every public library, right, or every other Federal facility across the board, which is why that tailoring actually would matter for Fourth Amendment purposes, with exceptions built in for certain sites as well as along the border itself.

Senator MOODY. Thank you, Mr. Chairman.

Chairman GRASSLEY. Senator Schmitt.

Senator SCHMITT. Thank you, Mr. Chairman. And I note that a couple of witnesses brought up some of the potential First Amendment concerns related to drones and monitoring activities. And Ms. Daskal mentioned specifically that she wanted to make sure she was ensuring people could engage in First Amendment-protected activity. And it's this sort of line of questioning I'd like to pursue with you. Did you, in your time at DHS, co-chair the Biden administration's Disinformation Governance Board?

Ms. DASKAL. I—no, I was not the co-chair of the governance——

Senator SCHMITT. Did you write the charter?

Ms. DASKAL. I—in my time at DHS, I was—at the time, I was the acting general counsel at DHS.

Senator SCHMITT. Well, I have a memo here from you with a couple things that we're going to get into, but you wrote the charter, correct?

Ms. DASKAL. I was, as I said, Senator—I was in a general counsel role, and in that role, everything came through my——

Senator SCHMITT. Did you have a role in picking Nina Jankowicz to be the executive director of the Disinformation Governance Board?

Ms. DASKAL. I was not the hiring authority.

Senator SCHMITT. Did you have input before she became Mary Poppins? Were you aware that she was going to become the executive director of the Disinformation Governance Board?

Ms. DASKAL. I was aware, yes.

Senator SCHMITT. Okay. Did you support that?

Ms. DASKAL. I am not going to get into internal conversations about——

Senator SCHMITT. Okay. Well, we'll get into—how about some public documents, here? Actually, let's just get into the memo that you authored. On January 31, 2022, you authored a memo to Secretary Mayorkas, asking him to sign off on the charter that you authored. In that charter, there's a few things that you were trying to address to dispel—as it relates to misinformation or disinformation relating to the origins and effects of COVID–19. Is your position that it would've been appropriate for the Government to work with social media companies to censor points of view that maybe COVID–19 originated in China?

[Poster is displayed.]

Ms. DASKAL. Senator, it's my view that it's not appropriate for the Government to censor any points of view.

Senator SCHMITT. Literally, you were a part of the Disinformation Governance Board of the United States of America. My contention is: The Orwellian name of Ministry of Truth was already taken, so the Disinformation Governance Board slid right in. And you were a big part of this. I mean, you wrote the charter. It also wanted to censor views—dispel disinformation about the efficacy of masks, another conspiracy theory that the Government thought it was their job to dispel.

And so I find it kind of rich that you're here expressing concerns about—First Amendment concerns about anything. A Federal district court judge said this was the biggest affront to the First Amendment in the history of the United States of America, this censorship enterprise that the Biden administration engaged in, that you were a big part of.

I want to ask you also about—in that memo that you wrote, attached to the charter, there is a proposed time schedule with Twitter for April 28, 2022. You were going to meet with Twitter executives, including Yoel Roth, who—the head of site integrity, to discuss—it's noted that Nick and Yoel both know the Disinformation Governance Board director, Nina Jankowicz, and the purpose was for them to become more involved with the Disinformation Governance Board analytic. Were you at that meeting?

Ms. DASKAL. I do not recall that meeting.

Senator SCHMITT. You don't recall? Well, it turns out that Twitter actually became very involved in your efforts, didn't they?

Ms. DASKAL. I was not engaged with Twitter on these efforts.

Senator SCHMITT. Okay. Well, they were engaged in helping dispel the Hunter Biden laptop as "a hack-and-leak—Russian hack-and-leak operation," which was cited, by the way, in the charter of things to address. COVID–19 conspiracy theories—I just think—I don't have a lot of time, and there's a—we could do a whole hearing on this, but as Missouri's Attorney General, I happened to bring the lawsuit *Missouri v. Biden*, which is why I'm so familiar with your efforts.

And I think that we would be remiss to not, at every point, point out the people who were involved in this, who would trample individual rights in this country, their ability to speak their mind because they thought the Government should decide what the truth was. And this country was founded on the principle that that's not the case; that individuals can make up their own minds. So, hope-

fully we never go down this road again, but you ought to be ashamed of yourself for your role in this.

Senator Moody [presiding]. Thank you, Senator Schmitt. Senator Cornyn.

Senator CORNYN. So, this topic caused the events of July the 13, 2024 to come to mind: the attempted assassination of President Trump, where the shooter used a drone in advance of the event to surveil the location of this program or this rally—and in a place that was supposed to be among the most protected in America, where temporary flight restrictions were in place. The Secret Service apparently didn't have adequate anti-drone technology or the know-how to actually stop these drones. So, to me, that just demonstrates that nowhere is safe. And, Mr. Dixon, you've made that point several times.

I want to ask Captain Wilson—Captain Wilson, thank you for your service to our State over many years. Obviously this is a big challenge at the Texas-Mexico border, and of course the Department of Public Safety—you're a Texas Ranger, former DPS officer. DPS has had a lot of experience dealing with border security matters over many years, but what's the—can you give us a sense of the volume or the number of drone encounters that are seen at the border these days? Is this an occasional occurrence? Is it a daily occurrence? Is it an hourly occurrence? How frequent are the drone incursions?

Mr. WILSON. Thank you, Senator. It depends on the location.

Senator CORNYN. Right.

Mr. WILSON. In a 12-month period, there were a little over 1,200 drone incursions across the border that we detected on our sensors.

Senator CORNYN. That you knew of?

Mr. WILSON. That we knew of, and that's an important point to make note of—is that we knew of. It is just our sensors, not—we're not combining all of the U.S. Border Patrol, DEA, or anybody else's sensors, where we can have a common operating picture of what's going on down there on the border.

Senator CORNYN. Would that be helpful?

Mr. WILSON. It would absolutely be helpful. El Paso, UTEP, has a system out there that is very robust and very layered, and it will actually scare you if you look at what flights are crossing the border.

Senator CORNYN. It strikes me as bizarre that, after all these years with all the attention being given to the border—both in the failures of the previous administration's policies to deal with border security matters and then now—that we still lack the capability to know what all is coming across the borders. And I think that's a matter of urgent need for the Congress to address. This is, after all, an international border, and it's fundamentally the Federal Government's responsibility. I understand the State of Texas under Governor Abbott had to step up in the absence of Federal Government law enforcement, to try to fill the gap, but it's still a huge challenge.

Every time I have been to the border—and I've been there many times and welcomed many of my colleagues down there so they could learn, as I have, from the people who are on the ground there—I've always been told by Border Patrol that border security

is really a combination of three things. It's infrastructure; it's boots on the ground; and it's technology. But I take it from your testimony that the technology still isn't capable of filling this particular gap.

Mr. WILSON. Yes, sir.

Senator CORNYN. And if you go along the Rio Grande River, if you ride in one of the river boats that the Department of Homeland Security has or the DPS has, you'll see a number of scouts by the cartels and the coyotes, directing the movement of immigrants across the border, where they see an opening or an opportunity. Is that right?

Mr. WILSON. Yes, sir.

Senator CORNYN. And so these drones provide an enhanced ability to defeat the efforts by the Federal, State, and local law enforcement to secure the border?

Mr. WILSON. Yes, sir.

Senator CORNYN. So, let's talk briefly about the scourge of fentanyl. Fentanyl has taken tens of thousands of lives in America. It showed up in every community throughout the country. And the unfortunate characteristic of fentanyl is it's easy to make from chemical precursors, and it's relatively compact and easy to transport. But do drones currently transport fentanyl across the border?

Mr. WILSON. I'm not aware—personally aware of any, but I'm sure there are, and I know that there's been those instances where drugs and other things have been flown across.

Senator CORNYN. These drones are capable of carrying a significant payload, right?

Mr. WILSON. Yes, sir.

Senator CORNYN. Of whatever is put on the drone. And, to your knowledge, are the transportation of fentanyl across the border confined to the ports of entry, or do they also include the space between the ports of entry?

Senator MOODY. And we're past time, but I'll let you finish that question.

Mr. WILSON. Between the ports of entry. Yes, sir.

Senator MOODY. Thank——

Senator CORNYN. And not between——

Mr. WILSON. No, between——

Senator CORNYN. You say——

Mr. WILSON [continuing]. The ports.

Senator CORNYN [continuing]. Including——

Mr. WILSON. Between the ports——

Senator CORNYN. Okay.

Mr. WILSON [continuing]. Of entry. Yes.

Senator CORNYN. Thank you. Thank you.

Senator MOODY. Thank you, Senator Cornyn.

Senator CORNYN. Well, there's this strange myth out there that the movement of drugs is just across the ports of entry and not between the ports of entry, but that's not your experience, is it?

Mr. WILSON. No, sir.

Senator CORNYN. Thank you, sir.

Senator MOODY. Thank you, Senator. Senator Kennedy.

Senator KENNEDY. The bad guys are using drones. Does anybody disagree with that? Okay. And the Federal Government has the au-

thority to fight back, does it not? But State—nobody disagrees with that statement? Sure, Professor.

Professor DONOHUE. I would say within limits, yes. Within constitutional limits.

Senator KENNEDY. Okay. Do any of you disagree with giving State and local law enforcement the authority to fight back?

Professor DONOHUE. Again, within constitutional limits.

Senator KENNEDY. Okay. Tell me what your constitutional concerns are, Professor.

Professor DONOHUE. So, I have three primary concerns. The first has to do with the Fourth Amendment and the conditions under which a warrant is required and a general warrant is forbidden by the Fourth Amendment. So, in this particular case, it's——

Senator KENNEDY. Professor, before you give me one of your lectures, are you saying that we should require State and local law enforcement to get a warrant before they fight back?

Professor DONOHUE. It depends on the condition. So, in an exigent circumstance or something along the border——

Senator KENNEDY. I'm aware of the exceptions to the warrant requirement. But generally speaking, you want to require them to get a warrant?

Professor DONOHUE. Only for the search of a device or the seizure of property. There are also due process implications of that.

Senator KENNEDY. Okay. You started to mention another one of your objections.

Professor DONOHUE. First Amendment.

Senator KENNEDY. First Amendment. Okay. Any others?

Professor DONOHUE. Yes, I also have a State rights, a Tenth Amendment concern here, which is that States own the airspace adjacent to the land within their State that's not Federally owned, and the current Federal provisions don't recognize State sovereignty in that way.

Senator KENNEDY. So, you want to give State and local law enforcement the authority to fight back, but you want to list a whole lot of conditions. Is that a fair assessment?

Professor DONOHUE. Not a whole lot, but some. There needs to be a nexus to the facility; it can't be any drone, anywhere in America, if you're concerned about a particular facility, but right now it's too broad. There have to be acknowledgments of First Amendment concerns—so, for instance, limiting the covered facilities to the experience and logic test which the courts use for right of public access or prohibiting media bans across the board or removing—setting a time limit before and after special events, so they don't extend extensively. This is what a number of State measures already do, and I'd like to see that at a Federal level and applied to bring this within the constitutional limits.

Senator KENNEDY. Sounds like a lot of conditions to me.

Professor DONOHUE. No, not very many. As long as there's probable cause and the conditions are met, then absolutely you can——

Senator KENNEDY. Have you ever heard——

Professor DONOHUE [continuing]. Search.

Senator KENNEDY [continuing]. Of a legislative practice called loving a bill to death?

Professor DONOHUE. Yes.

Senator KENNEDY. Okay. And that's when you take a bill, and somebody says, I'm really for this bill, but then they add so many amendments and they screw it up so badly that the bill either becomes ineffective or doesn't pass. Is that a pretty accurate description?

Professor DONOHUE. Of the term?

Senator KENNEDY. Yes.

Professor DONOHUE. Yes.

Senator KENNEDY. You're trying to love this to death, aren't you?

Professor DONOHUE. I disagree.

Senator KENNEDY. You're not really for giving law enforcement the power to fight back, are you?

Professor DONOHUE. I am in favor of giving law enforcement that power and respecting constitutional limits.

Senator KENNEDY. I don't believe you, Professor. Okay. You're not talking to Bambi's baby brother, here. Okay. I've read some of your stuff. I think you'd be more intellectually honest if you'd just come out and say, I'm on the side of the bad guys here. I think we shouldn't give State and local law enforcement the authority to fight back. You're trying to make it as hard as possible, aren't you?

Professor DONOHUE. We'll have to disagree on that point, Senator.

Senator KENNEDY. Nah. You ever heard the expression, watch what they do, not what they say? I've watched what you've done. I know what you believe. Were you—you're on the FISA Court?

Professor DONOHUE. I'm not on the court, no. I'm an amicus for the Foreign Intelligence Surveillance Court and the Court of Review.

Senator KENNEDY. Okay. Were you there when you guys issued all those bad warrants against Trump's people?

Professor DONOHUE. I can't discuss my work on the court, unfortunately.

Senator KENNEDY. Oh, it's top secret. Right. I'd be—you'd have to put me on double—the American people on double secret probation if you told them the truth, wouldn't you?

Professor DONOHUE. No. I can't discuss my matters that I've handled before the court. I can discuss the public ones, where I've dealt with First Amendment concerns and the right to petition. I did an extensive history looking——

Senator KENNEDY. I'm done.

Professor DONOHUE [continuing]. At that right——

Senator KENNEDY. I'm done——

Professor DONOHUE [continuing]. To petition.

Senator KENNEDY [continuing]. Madam Chair.

Senator MOODY. Thank you. Thank you, Senator Kennedy. We're going to turn it over to Senator Blumenthal.

Senator BLUMENTHAL. Thanks, Madam Chair. You know, when there're sightings or reports of drones, the ones who respond are often the local and State police; law enforcement, as you know. And very often DHS or the Department of Justice take a lot longer to respond, and the ones on the line—as we've seen recently in Connecticut, reports, sightings, many of them—and they often lack the resources, really, to provide adequate answers. Shouldn't we be

providing more authority and resources to local and State law enforcement?

The FAA, right now, is strained as it is. I don't need to tell anyone in this room. Can barely provide for air safety. In fact, as we've seen, is losing the skilled workforce that it needs to protect safety in the skies. Shouldn't we be giving more authority to local and State law enforcement, along with the resources to do their job? Let me ask all of you that question. And maybe be more——

Mr. WILSON. Yes.

Senator BLUMENTHAL [continuing]. Specific——

Ms. DASKAL. Yes.

Senator BLUMENTHAL [continuing]. About what specific equipment should be provided and how it should be provided.

Mr. DOOLEY. Again, that's a question that, again, some of our four Federal partners—our Federal partners that are allowed to do this; they've been doing it longer; they've had more capabilities than us—again, like my earlier statement, I think that it should be training, number one. Rules and regulations. Someone should not only be fluent with how the technology works but also FAA rules and regulations, privacy concerns, et cetera, so that when they make that decision to not only detect but mitigate, it's done correctly or as correctly as a human being can make that decision. But I think that that's how you move forward.

And yes, they should have the ability, but it should be under certain guidelines and restrictions, that they need certain levels of training, certification, education, et cetera, to make sure that when they do detect something, they're making the right decision, based on a multitude of different things to either mitigate it or shoo it away. It should be done in that way.

Ms. DASKAL. I agree, as well, Senator. I think it is also important that State and local authorities, as well as airport owners and critical infrastructure owners, are given the authority to engage in advanced detection measures, which they currently do not have, so that there is a common understanding and awareness of threats before it becomes too late. There also should be an expansion of authority to trained State and local authorities—subject to oversight; subject to protections for civil rights, civil liberties, and privacy—that would allow trained State and local authorities to engage in appropriate mitigation measures. And, finally, there needs to be, as well, the ability for our domestic drone industry to test and innovate and be able to do the kind of testing to ensure that the Federal Government and State and locals have the best technology to engage in, ideally, the kind of disruptions that don't require kinetic action, as well.

Senator BLUMENTHAL. Are you concerned about how robust the domestic drone industry is?

Ms. DASKAL. I think it is important to support the domestic drone industry, and I also think it's important to ensure that, as entities within the domestic drone industry are seeking the opportunity to engage in the testing, that that is facilitated so that the drone industry is a step ahead of the adversaries.

Senator BLUMENTHAL. The overwhelming number of drones used in this country are made abroad, correct?

Ms. DASKAL. Yes. That is a concern.

Senator BLUMENTHAL. In China?

Ms. DASKAL. That is a concern, sir.

Senator BLUMENTHAL. What is the percentage? You may have already testified to it, and I apologize for repeating.

Professor DONOHUE. If I may, 80 percent of the drones are DJI, which is a Chinese-owned company.

Senator BLUMENTHAL. Eighty percent. And what can be done to increase the number made in this country and perhaps restrict the number made in China? Mr. Wilson?

Mr. WILSON. Yes, sir, Senator. I'm going to echo what my partner here has said already. Increase the funding for American drone manufacturers to not—to be competitive in technology and price. They can do it. They just haven't.

Senator BLUMENTHAL. With increased funding.

Mr. WILSON. Yes, sir.

Senator BLUMENTHAL. Thank you.

Senator MOODY. Thank you, Senator Blumenthal. Senator Blackburn.

Senator BLACKBURN. Thank you, Madam Chairman, and thank you all for being here. And I think to each of us, when you look at DJI, their numbers are of tremendous concern for us. That's why some of us have had provisions that remove the ability of our military to use DJI drones, and also for local law enforcement, from them using DJI drones. Any of these drones that are manufactured by adversaries or in these adversarial situations are a safety risk to us because of the transmission of that data and then who holds that data and where they hold that data.

So, as we continue to push back on utilization of foreign-manufactured drones, it gives openings for the domestic industry to increase their presence. And we hope, Mr. Wilson—in answer to or in addition to what you were saying, we hope that this helps to motivate domestic manufacturing of these drones. We do know there are some supply chain issues around that, and as we look at tariffs and trade we are seeking to address some of those issues.

I represent Tennessee. We have a lot of outdoor events in Tennessee. We've got Titans football that people enjoy; we've got the Bonnaroo Music Festival and so many festivals around our State. I've recently done the Fish Fry and the Strawberry Fest and a couple of others in our beautiful State. But one of the things people are concerned about is when they do hear that drone flying overhead, because they don't know who put it there and why they put it there and if this is an infringement on their privacy or if they are being spied upon or—and the first person they turn to is going to be local law enforcement.

And I agree with some of you and disagree with Professor Donohue. I think it's an imperative that we give local and State law enforcement the ability to participate in this policing and the mitigation efforts that need to take place. I would like—and Sergeant Dooley, let me come to you on this. Let's break this down and look at what kind of partner the FBI and the FAA have been for State and local law enforcement. As you look at these mitigation efforts, what kind of partner are they when it comes to these counter-UAS efforts? And where could that relationship be strengthened?

Mr. DOOLEY. Number one, the relationship—the stakeholder relationship we have with both of those entities is pretty strong. The FAA is super supportive; unfortunately, they can't grant those permissions to do those things. Even some of the data that some of our Federal partners at times collect—they're worried about, like, how it was collected, et cetera. But it can be strengthened by, again, just starting the process of establishing one of those Federal entities as the lead to help guide people forward. And then from there I think it'll just blossom and organically grow into something much stronger, where there is regulation: Now we have a pathway forward. Now people can start learning how to do this.

And again, I'm a strong believer that you shouldn't just understand the technology itself. You should have a firm grasp on everything that goes into it, including FAA rules and regulations, et cetera, so that when you have one of those events in Tennessee, you know, if someone had a legal right to be there, fair and equitable access to that airspace they're up, they have the proper permissions or whatever the case is, and they're just documenting or taking photos or whatever it is, it doesn't mean that we shouldn't know that that's something benign versus something that's bad.

Senator BLACKBURN. So, basically a pre-clearance——

Mr. DOOLEY. Yes.

Senator BLACKBURN [continuing]. To be in that space?

Mr. DOOLEY. Yes.

Senator BLACKBURN. Okay. Thank you for that. I want to move on to something—Mr. Dixon had talked about this earlier. And, Sergeant Dooley, I'll stay with you. We've had two instances in Tennessee where a criminal attempted to use an armed drone to murder someone. And in one case, there was somebody that was planning an attack on the Knoxville FBI field office, and in another a man attempted to attack an electronic substation with homemade drones. So, we know that this takes place. And Mr. Dixon talked about it with law enforcement and prisons and jails. So, it just leads me to believe that there has got to be some reforms on how we look at the regulations around the drones.

And I know I am over time. Madam Chairman, if I may take a moment—and, Sergeant Dooley, let me have you talk a bit—how we do these reforms, before there is a successful attack that is carried out from—how would we go about those reforms so we're in front of any type attack that takes place?

Mr. DOOLEY. Again, we have three handsome public safety professionals; we have our Senators here, decisionmakers; and we have some legal experts. I mean, there's a pathway forward. It can be quick. It can be done correctly. But again, I'm a firm believer that we have to establish someone who's the lead, and then from there I think that we can move forward to get it done pretty quickly. And then, of course, all of our States represented here—Florida and Texas—it would obviously step up to whatever level we would need to, to make it happen in a timely fashion.

Senator BLACKBURN. Okay. Secretary Dixon, anything to add on that?

Mr. DIXON. I agree. The frustrating thing is the technology exists. That's not our problem. It's the authority we need. So, that's good news and bad news. The technology's there to do everything

we need to do. I would distinguish ourself a little independently in the corrections industry, because we are a fixed site and we have a different population, so I don't think there's any reason we can't work together to move ahead on authorities we need to combat this immediately.

Senator BLACKBURN. So, the Federal, State, and local partnership—we need to work through that?

Mr. DIXON. Yes. The partnership is great. We need the congressional—we need language, authority from the Federal level, to allow us to utilize the tools.

Senator MOODY. Thank you, Senator Blackburn. And thank you to all of our witnesses for being here today. I know this was a long hearing, but I appreciate your attention and participation throughout. Written questions can be submitted by Senators for the record until May 27 at 5 p.m., and then we'll ask the witnesses to respond and return the questions to the Committee as quickly as possible.

Senator MOODY. With that, you are free to go and enjoy lunch. The hearing is adjourned.

[Whereupon, at 11:57 a.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

Written Testimony of Jennifer Daskal[1]

Before the United States Senate Committee on the Judiciary

Hearing on "Defending Against Drones: Setting Safeguards for Counter Unmanned Aircraft Systems Authorities"

May 20, 2025

Chairman Grassley, Ranking Member Durbin, and distinguished Members of the Committee, thank you for inviting me to testify at today's hearing, *Defending Against Drones: Safeguards for Countering Unmanned Aircraft Systems Authorities.*

The safety and security of Americans from the potential misuse of drones[2] is a critically important issue—one that should be top of mind for every American.

Drone safety issues rose to prominence during the last two months of 2024, when there were numerous reports of suspicious drones flying over New Jersey.[3] At the time, I was the Deputy Homeland Security Advisor. Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), the Federal Aviation Administration (FAA), and Department of Defense (DOD) officials surged resources to assess what was happening in the New Jersey skies. Agencies sent advanced detection technology and trained visual observers to support local officials in New Jersey.[4] FBI set up a tip line.[5] FAA imposed flight restrictions around power stations, critical infrastructure facilities, and other locations across New Jersey. For several weeks, I held almost-daily meetings with relevant Departments and Agencies to make sure we were doing what we could, within the scope of our limited authorities, to support New Jersey. But there were significant constraints—as a result of insufficient authorities and resources—in what the federal government could do.

FBI, DHS, FAA, and others reviewed the reports that came in. They did not find any evidence of malicious activity, foreign involvement, or criminal action. Instead, the reviews of reported drone sightings revealed that many were lawfully present aircraft and helicopters; others were

---

[1] I formerly served as the Deputy Homeland Security Advisor (2023-2024), National Security Council Principal Deputy Legal Advisor (2023) and Acting General Counsel and Principal Deputy General Counsel at the Department of Homeland Security (2021-2023). Currently, I am a Partner at Venable, LLC. I am offering this testimony solely in my personal capacity. I am not offering views on behalf of Venable or any of Venable's clients. I have not received any compensation or any other benefit for providing this testimony.

[2] For the purposes of this testimony, I am using the words "drones" and unmanned aircraft" interchangeably to refer to aircraft that can be operated remotely, with or without human involvement.

[3] Dave Collins, "Mystery drone sightings continue in New Jersey and across the US. Here's what we know," *Associated Press*, Dec. 20, 2024, https://apnews.com/article/drones-new-jersey-what-to-know-e6f565f5d51d9d47ad140e7e7d131842; Tom Winter and David Li, "FBI investigates mysterious drones filling night sky in New Jersey that have 'unnerved' residents," *NBC News*, Dec. 3, 2024, https://www.nbcnews.com/news/us-news/fbi-investigates-mysterious-drones-filling-night-sky-new-jersey-unnerv-rcna182637.

[4] "DHS, FBI, FAA & DoD Joint Statement on Ongoing Response to Reported Drone Sightings," Dec. 17, 2024, https://www.faa.gov/newsroom/dhs-fbi-faa-dod-joint-statement-ongoing-response-reported-drone-sightings.

[5] "FBI Newark Seeks Information on Drone Sightings," Dec. 3, 2024, https://www.fbi.gov/contact-us/field-offices/newark/news/fbi-newark-seeks-information-on-drone-sightings.

lawfully present drones.[6] In early January 2025, the Trump Administration reached a similar conclusion. In President Trump's words, as conveyed via his press secretary: "The drones that were flying over New Jersey in large numbers were authorized . . . this was not the enemy."[7]

But the fear at the time was palpable. And justified. Drones serve key public safety, recreational, and commercial functions. But they also can be weaponized by malicious actors, in ways that put Americans at risk. Even non-malicious uses of drones—including the careless flying of drones into protected airspace—poses significant risk to aviation safety. The current patchwork of authorities is insufficient in light of these risks.

In April 2022, the prior Administration, in recognition of the current vulnerabilities, submitted to Congress a legislative proposal that would have expanded the authorities and set of actors who could respond to the risk posed by the misuse of drones. Bipartisan legislation repeatedly offered by Senators Gary Peters (D-MI) and Ron Johnson (R-WI)—including most recently, the "Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2024," offered as an amendment to the National Defense Authorization Act of 2025—would also expand and extend current authorities in critically-needed ways.[8] To date, Congress has failed to act. It is time to do so now, before it is too late.

In the remainder of this testimony, I will do three things. I will address: (i) the current state of play with respect to the use of drones, the risk of misuse, and current counter-drone authorities; (ii) the gaps in these authorities, in light of the risks; and (iii) what is needed to responsibly protect Americans from the potential misuse of drones, in a manner that protects civil rights and civil liberties.

I. The Current State of Play

There are over one million drones registered with the FAA in the United States—a number that is predicted to grow to 2.7 million by 2027.[9] The vast majority of these drones are used for commercial, recreational, and other lawful purposes, serving highly valuable functions which should be actively supported. But as drones proliferate, the risks increase as well. This section lays out: (i) the benefits of drones, as well as their risk of misuse; (ii) the key detection and mitigation tools needed to identify and counter threats that arise; and (iii) the current, and limited, scope of authorities to do so.

---

[6] Andrea Shalal & Ryan Patrick Jones, "FBI, White House find no evidence of security threat in New Jersey drone sightings," *Reuters*, Dec. 13, 2024, https://www.reuters.com/world/us/no-evidence-new-jersey-drone-sightings-pose-security-threat-white-house-says-2024-12-12/.

[7] Stacey Dec, "Trump says NJ drones were 'authorized after suggesting Biden kept public 'in suspense," *ABC News*, Jan. 28, 2025, https://abcnews.go.com/Politics/leavitt-reveals-nj-drones-authorized-faa-white-house/story?id=118187426.

[8] S. Amdt. 3233 to S.4638: Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2024, submitted Aug. 1, 2024, https://www.congress.gov/amendment/118th-congress/senate-amendment/3233.

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

The Benefits of Drones and The Risk of Misuse

Drones serve key functions. Drones are used to support firefighters, the delivery of life-saving aid, critical infrastructure management, agricultural production, military operations, along with multiple other commercial and recreational uses.[10] As the technology supporting unmanned aircraft systems advances, drones will be able to do even more. It is critical that we support and help grow our domestic drone industry, which plays a key role in the current economy.

But they also carry risk. One needs to read only a few headlines about the fighting in Ukraine and across the Middle East to know that drones—many of which are off-the-shelf technologies that have been adapted for war—are at the forefront of military conflict.[11] Drones have been used in assassination attempts, including of the President of Venezuela and Prime Minister of Iraq.[12] Transnational criminal organizations use drones to smuggle deadly drugs across our southwest border.[13] Drones can be used by foreign adversaries for espionage purposes, including to collect intelligence on targets of interest.[14] Drones have also posed serious safety risks to airports, critical infrastructure, and large public gatherings like football games.[15]

In fact, just last week, on May 13, the Department of Justice arrested a 19-year-old, former member of the Michigan Army National Guard for planning to conduct a mass-shooting at a Michigan military base on behalf of the Islamic State of Iraq and al-Sham (ISIS). At the time of

---

[10] Michelle Putz, "Drones help make fighting fires safer, cheaper, better throughout Rocky Mountain Region," *U.S. Forest Service*, Nov. 5, 2024, https://www.fs.usda.gov/inside-fs/delivering-mission/deliver/drones-help-make-fighting-fires-safer-cheaper-better; "Using drones to deliver critical humanitarian aid," *United Nations World Food Programme*, https://drones.wfp.org/updates/using-drones-deliver-critical-humanitarian-aid; Dr. Ibrahim Odeh et al., "The Sky's the Limit: Leveraging Drone Technology in Infrastructure Projects," *Global Infrastructure Hub*, Feb. 20, 2024, https://www.gihub.org/articles/the-skys-the-limit-leveraging-drone-technology-in-infrastructure-projects.

[11] Marc Santora et al., "A Thousand Snipers in the Sky: The New War in Ukraine," *The New York Times*, March 3, 2025, https://www.nytimes.com/interactive/2025/03/03/world/europe/ukraine-russia-war-drones-deaths.html (citing the chairman of the defense and intelligence committee in Ukraine's Parliament for the claim that drones account for some 70% of deaths and injuries in the Russian-Ukrainian war); Lolita Baldor, "Houthi rebels have shot down 7 US Reaper drones worth $200 million in recent weeks," *Associated Press*, April 24, 2025, https://apnews.com/article/houthis-us-warships-red-sea-e6e97a7131c48640ccf74b1916628234.

[12] Colin Clarke, "Approaching a 'New Normal': What the Drone Attack in Venezuela Portends," *RAND*, Aug. 13, 2018, https://www.rand.org/pubs/commentary/2018/08/approaching-a-new-normal-what-the-drone-attack-in-venezuela.html; John Davison and Ahmed Rasheed, "Iraqi PM safe after drone attack on residence, military says," *Reuters*, Nov. 7, 2021, https://www.reuters.com/world/middle-east/drone-attack-targets-iraq-pm-who-escapes-unhurt-iraq-military-2021-11-07/.

[13] Drug Enforcement Administration, "2017 National Drug Threat Assessment," Oct. 2017, https://www.dea.gov/sites/default/files/2018-07/DIR-040-17_2017-NDTA.pdf.

[14] Jordan Pearson, "The Unusual Espionage Act Case Against a Drone Photographer," *WIRED*, May 30, 2024, https://www.wired.com/story/fengyun-shi-espionage-act-drone-photography/.

[15] Aaron Kessler & Michael Biesecker, "Drones pose increasing risk to airliners near major US airports," *AP News*, April 21, 2025, https://apnews.com/article/drones-risk-airports-planes-safety-collisions-d8bb7192173d90b46258c91152454cf3; Stephon Dingle, "FBI warns drone pilots to stay away from M&T Bank Stadium ahead of Ravens vs. Steelers AFC Wild Card matchup," *CBS News*, Jan. 10, 2025, https://www.cbsnews.com/baltimore/news/ravens-vs-steelers-drone-pilots-afc-wild-card-game-fbi-m-t-bank-stadium/.

the arrest, which was the day of the scheduled attack, the 19-year-old had already launched a drone in support of the attack plan.[16]

Even non-malicious uses of drones pose potential threats. Operator negligence or error can have deadly consequences, as exemplified by the crash between a drone and a lifesaving firefighting aircraft in Los Angeles early this year.[17] According to one report, drones accounted for some two-thirds of near midair collisions with commercial passenger planes, each of which could have led to catastrophe.[18] As the use of drones proliferates, it will become increasingly important to deconflict the airspace and protect against even inadvertent incursions into protected airspace and flight paths.

As the nature of warfare evolves, it is critical that the United States have the best—and safest—technology to fight in this new domain. But we need to also be prepared for the threats posed by both malicious and careless uses of drones, both in conflict areas and in the homeland. That requires, at a minimum, an extension and expansion of current counter-drone authorities to better equip the federal government, as well as trained state, local, territorial, and tribal authorities to detect, and, as appropriate, consistent with safeguard for safety, civil rights and civil liberties, respond to threats.

Detection and Mitigation Tools

Effectively responding to these threats—whether the result of error, negligence, or malice—requires both the ability to *detect*, and, when appropriate and needed, to *mitigate* the threat. A patchwork of federal and state laws, including those related to aircraft piracy, interception of electronic and wire communications, and computer fraud and abuse, makes it unlawful to engage in most detection measures—including any measure that involve recording or decoding signals between a drone and its operator—and in mitigation measures, without express statutory authorization to do so.

Detection systems rely on a variety of technologies, including radio frequency, electro-optic, infrared, and acoustic sensors. Certain passive technologies, such as those that identify electromagnetic pulses or light emitting from drones do not require affirmative authority under federal law, but any technology that records or decodes signal information between a drone and its operator likely runs afoul of the Pen Trap/Trace statute, absent a specific authorization.[19]

Mitigation measures include the capability to disrupt, disable, seize, and destroy an unmanned aircraft system to avoid harm—and require affirmative authority prior to use. Such measures

---

[16] U.S. Department of Justice, Office of Public Affairs, "Michigan Man Arrested and Charged with Attempting to Attack Military Base on Behalf of ISIS." May 14, 2025, https://www.justice.gov/opa/pr/michigan-man-arrested-and-charged-attempting-attack-military-base-behalf-isis.

[17] U.S. Department of Justice, U.S. Attorney's Office, Central District of California, "Culver City Man Agrees to Plead Guilty to Recklessly Crashing Drone into Super Scooper Firefighting Aircraft During Palisades Fire," Jan. 31, 2025, https://www.justice.gov/usao-cdca/pr/culver-city-man-agrees-plead-guilty-recklessly-crashing-drone-super-scooper.

[18] *See* Kessler & Biesecker, *supra*, note 15.

[19] *See* 18 U.S.C. § 3121 (prohibiting the use of a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, absent the application of specified exceptions).

include non-kinetic activities, such as jamming a drone's radio or GPS signals and taking over the control of a drone from its operator. They also include kinetic activities, which involve physically destroying or disabling a drone by taking it down, *i.e.*, with a projectile, laser, or net.

Kinetic actions pose their own set of risks—some potentially fatal—and should be used as a matter of last resort. In New Jersey, for example, multiple manned aircrafts were mistaken for unmanned drones; use of a projectile to take down those reported drones likely would have caused fatalities. Even when there is certainty as to the nature of the target (*i.e.*, that it is a drone) and intent (*i.e.*, that it is malicious), kinetic actions risk collateral damage to people and property in the vicinity, depending on where the downed drone and drone parts land.

Current Authorities to Engage in Counter-Unmanned Aircraft (C-UAS) Actions

Currently, only four federal agencies have the authority to engage in advanced detection and mitigation measures in response to threats posed by drones: DOD, Energy (DOE), DHS, and Justice (DOJ). These agencies have *limited* authorities to provide protection over "covered" facilities and assets, as described below:

- **DOD** has limited authority to engage in advanced detection and mitigation measures, in the event of a threat to a Secretary of Defense-designated covered facility or asset.[20] Covered facilities or assets must be identified on a "risk-based assessment," and must relate to one of nine DOD-identified missions, including nuclear deterrence, missile defense, and protection of the President and Vice-President.[21]

  A key subset of these authorities—*i.e.,* those related to the protection of the President and Vice-President, air defense of the United States, combat support agencies, special operations activities, and production and storage of high-yield explosive munitions—expires at the end of 2026, absent Presidential or Congressional action.[22]

- **DOE** has limited authority to engage in advanced detection and mitigation measures to protect a Secretary of Energy-designated facility or asset that stores or uses special nuclear materials.[23]

- **DHS and DOJ** also have limited authority to engage in advanced detection and mitigation measures to protect Secretary of Homeland Security and Attorney General covered facilities that are deemed "high risk and a potential target for unlawful unmanned aircraft activity" and meet specified criteria.[24]

  - DHS authority extends to those designated assets and facilities that directly relate to the security or protection functions of Customs and Border Protection (such as disrupting the movement of illicit drugs across the southwest border), Secret

[20] *See* 10 U.S.C. § 130i.
[21] *Id.* § 130i (j)(3).
[22] *Id.* § 130i (i)
[23] *See* 50 U.S.C.§ 2661.
[24] *See* 6 U.S.C. § 124n.

Service operations (such as the protection of the President); and protection of federal property.[25]

- DOJ authority extends to personal protection operations by the FBI and U.S. Marshals Service; protection of correctional facilities; and protection of the courts.[26]

- DHS and DOJ both also have authority to provide protection for a National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) event;[27] specified mass gatherings, based on a governor's request; an active Federal law enforcement investigation, security function, or emergency response; and certain U.S. Coast Guard Operations.[28]

Although the FAA has statutory responsibility to provide for the safety and efficiency of the national airspace, it does not have general C-UAS authority—despite receiving over 100 reports of unmanned aircraft near airports each month.[29] That said, under the 2018 FAA Reauthorization Act, FAA was given limited authority to deploy advanced detection and mitigation systems at five airports for purposes of "evaluating and testing unmanned aircraft detection and mitigation systems;" in 2024, Congress extended that authority to cover "any other location that the [FAA] Administrator deems appropriate."[30]

Airports can nonetheless employ passive detection authorities that do not trigger the criminal prohibitions found in the Pen/Trap statute or other federal or state laws. That said, passive detection provides only limited assistance to airports, and there is also significant confusion about the scope of what is permitted. In some cases, airport operators have refrained from putting in place any detection measures as a result.[31]

II. The Key Gaps in Authority

The current authorities permit federal agencies to provide key protections to people and places, including to the President and Vice-President; the Macy's New Year's parade; the Super Bowl; World Series; Boston marathon; and presidential inaugurations, among many other events and

---

[25] *Id.* § 124n(k)(3)(C)(i).

[26] *Id.* § 124n(k)(3)(C)(ii).

[27] NSSE events are major federal government or public events, such as presidential inaugurations and the yearly State of the Union address; SEAR events are pre-planned special events, such as the Super Bowl, that do not generally rise to the level NSSEs, but are nonetheless determined by the Secretary of Homeland Security to justify federal support, based on submissions from federal, state, and local authorities and risk-based authorities

[28] *See* 6 U.S.C. § 124n(k)(3)(C)(iii).

[29] *See* FAA "Drone Sightings Near Airports," Federal Aviation Administration, uhttps://www.faa.gov/uas/resources/public_records/uas_sightings_report.

[30] *See* 49 U.S.C. § 44810(c); FAA Reauthorization Act of 2018, Pub. L. No. 115-254, § 383 (2018); FAA Reauthorization Act of 2018, Pub. L. No. 115-254, § 904 (2018).

[31] *See* Government Accountability Office, "Aviation Safety: Federal Efforts to Address Unauthorized Drone Flights Near Airports," at 13, March 2024, https://www.gao.gov/assets/d24107195.pdf.

locations.[32] The Bureau of Prisons relies on the DOJ C-UAS authority to protect against drones bringing weapons and other contraband into its facility. DHS uses its authority to counter the flow of fentanyl into our country.

But there are key gaps in the authorities, most notably with respect to protection of airports; critical infrastructure; and mass gathering events, including large sporting events, that do not currently qualify for federal protection. While federal agencies are well-positioned to plan for a limited number of pre-identified situations, they are not well-equipped to either identify or respond quickly to emergent threats. The federal government also lacks the personnel and resources to protect every major sporting event, concert, or other event where there are large numbers of people gathered that are vulnerable to threats from the misuse of drones. The current short-term sunset clauses in the DOJ, DHS and DOD authorities exacerbate this challenge—making it difficult for federal agencies to engage in the kind of long-term budget planning and preparation needed to ensure sufficient investments in technology and personnel to support the C-UAS mission. Short-term sunset clauses also mean a continuous risk of a lapse in the current authorities, which would put Americans' safety at risk.

The following delves into each of these gaps in authority in more detail.

- *Airports:* As described above, some airports engage in passive detection, while others are deterred from doing so based on the lack of legal clarity as to what is permissible. The federal government also lacks authority to engage in persistent C-UAS measures at airports. Yet, the threats to civil aviation posed by both careless and malicious drone operators persist.

- *Critical infrastructure:* Our electric grid, power plants, water and wastewater systems, and chemical sector are poorly protected by the current mix of authorities—and in many cases not protected at all. It is important that we protect our critical infrastructure from the combination of surveillance and disruptions that even simple, off-the-shelf drones could cause, via added cameras or payloads.

- *Public Gatherings:* Current law provides potential protections for certain high-profile mass gatherings, including National Special Security Events, and when requested by a Governor and subject to a risk-assessment and the availability of limited technologies and personnel to provide protections at such events. Meanwhile, just about every sporting event, outdoor concert, or political rally provides a setting that a malicious actor could exploit. Neither the current authorities nor the available resources are sufficient to provide needed protections in such settings.

- *Sunset clause:* The initial 2018 DOJ and DHS authorization to engage in C-UAS activities was set to expire on October 5, 2022. Since then, the DOJ and DHS C-UAS authorities have been the subject of eight different extensions—often for just a few months at a time. The current authorization expires in just a few months, on September

[32] Brad Wiegmann and Robert Wheeler, "Statement Before the Committee on Homeland Security," at 5, Dec. 10, 2024, https://homeland.house.gov/wp-content/uploads/2024/12/2024-12-10-CTITMS-HRG-Testimony.pdf. (describing UAS detection and protection operations conducted by the FBI between 2018 and 2024).

30, 2025. The potential lapse in authorities creates uncertainty, making it difficult to justify the kind of investments in technology and personnel needed to adequately address the potential threat posed by a combination of careless and malicious use of drones.

- *Cross-Agency Support*: Current law gives each of the agencies authorized to engage in C-UAS activities specific lanes in which to operate. FBI cannot support a DHS or DOD mission, and vice-versa—even if the FBI has technologies and personnel in place to provide the most immediate protection in the wake of an emerging or urgent threat.

- *Growing state and local needs*: Critically, even with a significant expansion of authorities and resources, federal agencies will not be positioned to address the growing demand for increased protection. State, local, territorial, and tribal (SLTT) authorities should, subject to safeguards, training, and oversight, be empowered to engage in advanced detection and certain mitigation measures. This would allow local authorities to, among other things, provide protections at currently unprotected sporting events and other large gatherings across the country, and respond to situations like that which emerged in New Jersey at the end of 2024. Properly vetted owners of airports and critical infrastructure should be authorized to put in place advanced detection measures as well.

III. Way Forward

In the short term, congressional action is urgently needed to make permanent the existing C-UAS authorities—or at least extend them for multiple years at a time, so as to protect against the uncertainty of a constantly-pending sunset Congressional action. Congressional action is also urgently needed to expand the existing authorities in order to better protect the American people from a known and evolving threat. It is essential that these authorities are subject to oversight and incorporate protections for civil rights and liberties, while also remaining nimble—so that needed detection and mitigation measures can be rapidly deployed in urgent situations, the available tools keep pace with current technological developments, and we remain a step ahead of our adversaries.

The bipartisan "Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act of 2024," offered last year by Senators Gary Peters and Ron Johnson, is a good starting point.[33]

The proposed legislation would do the following key things:

- *Expand federal coverage over airports, critical infrastructure, and large public gatherings:* The legislation would give DOJ and DHS explicit authority to engage in C-UAS activities to protect airports and critical infrastructure. It would also give DOJ and DHS expanded authority to support SLTT law enforcement agencies, including with respect to protection of mass gatherings, critical infrastructure, government buildings, and disaster response that is subject to SLTT jurisdiction.

[33] S. Amdt.3233 to S.4638, *supra*, note 8.

- *Cross-agency support:* The legislation would give DHS and DOJ authority to support one-another, DOD, and DOE in conducting their authorized C-UAS mission—thus helping to ensure the fastest and most effective deployment of resources in response to an emergent threat.

- *Expanded detection-only authority:* The legislation would give approved SLTT law enforcement officials, airport owners and operators, and critical infrastructure owners and operators limited authority to use authorized equipment, subject to review and oversight by multiple federal agencies, to engage in *detection-only* activities, subject to specified privacy protections—enabling broader coverage over currently unprotected locations and early detection of risks.

- *SLTT Pilot Program:* The legislation would create a limited pilot program—capped at six agencies in the first year and no more than thirty over five years—for SLTT law enforcement agencies to mitigate a credible threat to a covered asset or facility, subject to direct oversight by DOJ and strict reporting requirements. This is a key step forward in enabling appropriately trained SLTT officials fill critical gaps left by the limited resources and capacity of federal authorities to respond to potential threats.

Core Protections: Safety Considerations and Key Civil Rights and Civil Liberties Concerns

The legislation includes key safety protections and protections for civil rights and civil liberties. Prior to authorizing a C-UAS mission, the Secretary of DHS and the Attorney General conduct a "risk-based assessment," to include an assessment of potential safety concerns; potential for interference with wireless communications; and potential First and Fourth Amendment considerations. Personnel authorized to conduct C-UAS missions also must be trained and certified, including with respect to protecting privacy and civil liberties.

The legislation further includes core privacy protections, including the requirement that any communication from an unmanned aircraft is acquired *only to the extent necessary to support an authorized C-UAS activity* and maintained only for as long as necessary. The legislation explicitly requires that all detection and mitigation measures be conducted in accordance with the First and Fourth Amendment.

Some have, nonetheless, raised surveillance concerns to argue that these protections for civil rights and civil liberties are insufficient. But this claim appears based on a misunderstanding of what constitutes an authorized C-UAS activity. What is needed for detection purposes is broadly consistent with what is already required to be broadcast by the FAA's Remote Identification of Unmanned Aircraft Rule[34]—namely the identity (via a serial number and session ID), location and velocity of an unmanned aircraft, and the location of the control station; the location of the unmanned aircraft; and the aircraft's velocity.[35] When operators fail to comply with these requirements, it is critical that appropriately trained authorities are able to identify the location of a potential hazardous drone, and if necessary, employ take-over technology to respond to a threat. If law enforcement separately sought communications content, such as emails, texts, or

[34] See 14 C.F.R. § 89 *et seq* (2021).
[35] Id. § 89.305.

recording of voice calls, from drone operators, they would, consistent with the Fourth Amendment, need separate authority to do so.

Sunset Provision

The proposed legislation includes a five-and-half year sunset, including for the core DHS and DOJ authorities. This is too short. To ensure effective planning, funding, training, and deployment of personnel, and to avoid a situation in which these critical authorities risk lapsing, the core authorities should be extended at least a decade, if not longer.

IV. Conclusion

To end where I started, drones play a vital role in our economy, have important recreational value, and serve key roles in supporting the delivery of public services, including disaster relief, support for firefighters, and accident rescues. But their rapid proliferation and ease of deployment also poses risks—including threats from nation-state adversaries, terrorists, and criminals, as well as from careless and irresponsible operators. It is essential that Congress put in place the authorities needed to identify and respond to such threats, consistent with protections for civil rights and civil liberties, and in a manner that ensures the C-UAS tools are themselves used safely and effectively. The bipartisan "Safeguarding the Homeland from the Threat Posed by Unmanned Aircraft Systems of 2024" includes the key elements to do so.

The 2024 reported sightings in New Jersey turned out to be a false alarm. Next time we might not be so lucky. The time for Congress to act is now.

FOUNDED 1870

American Correctional Association

Advance. Connect. Achieve.

Statement for the Record

Defending Against Drones: Setting Safeguards for Counter Unmanned Aircraft System Authorities – May 20, 2025

By Ricky Dixon, 109th President of the American Correctional Association

United States Senate Committee on the Judiciary

My name is Ricky Dixon, and I serve as Secretary of the Florida Department of Corrections and currently serve as the 109th President of the American Correctional Association. I am honored to speak today on behalf of the American Correctional Association, which represents thousands of correctional professionals across the United States. Thank you, Chairman Grassley and Ranking Member Durbin, for holding this hearing on the urgent public safety threat posed by the criminal use of unmanned aircraft systems (UAS).

Drones have become one of the most dangerous and rapidly evolving tools used by organized criminals to penetrate the secure perimeters of our nation's correctional facilities. Drones are routinely being used to smuggle contraband, including fentanyl, heroin, razor blades and cell phones directly into prison yards and housing units. These incidents are not isolated; they are frequent and highly coordinated.

Organized criminal groups, including domestic gangs and transnational drug cartels, use drones to bypass traditional security systems and smuggle contraband that contributes to violence, drug distribution, and gang activity inside correctional facilities.

The consequences are immediate and severe. Facilities are experiencing overdose deaths from drone-delivered narcotics. Contraband cell phones delivered by drones are used by incarcerated individuals to coordinate gang violence, target witnesses, and orchestrate drug operations. Weapons smuggled in by drones have been used to commit serious assaults.

Most disruptive to correctional operations, however, is the institutional response required when a drone is detected. Any confirmed or suspected drone incursion triggers a full facility lockdown. This means all rehabilitative programming must be suspended, including educational classes, vocational training, substance use disorder treatment, and mental health services. Staff are redirected from therapeutic and rehabilitative functions to search for contraband. These disruptions are not brief. They can last for hours or even days. Repeated incidents undermine the long-term stability of a correctional environment and stall critical progress for individuals preparing for reentry into society.

The American Correctional Association has long supported bipartisan efforts to reduce recidivism, expand treatment, and support reentry success. We have been proud to back critical legislation such as the Second Chance Reauthorization Act and the Residential Substance Abuse Treatment (RSAT) for State Prisoners Reauthorization Act - both of which strengthen the continuum of care and provide vital programming inside correctional facilities.

But these programs cannot be fully effective in facilities where drone activity is constantly disrupting operations and flooding correctional facilities with narcotics and weapons.

Every time a drone breach forces a lockdown, educational and therapeutic services come to a halt, and incarcerated individuals miss opportunities for progress. Counter drone authority is not just about interdiction. It's about safeguarding the very programs Congress has worked hard to support.

And these disruptions come at a time when correctional agencies are already stretched to the limit. Across the country, we are facing significant recruitment and retention in some systems. In some facilities, staff are working mandatory overtime simply to maintain basic operations. The added burden of drone incidents, requiring all-hands responses, extended lockdowns, and increased security operations, further exhausts a workforce already operating under extreme strain. This is not sustainable.

Despite the seriousness of these threats, state and local correctional agencies remain legally prohibited from taking meaningful action against drones. Current federal law limits the use of counter-UAS technologies, such as signal jamming, tracking, and drone interdiction, to just four federal agencies. Even though correctional facilities are among the most frequent and vulnerable targets of drone activity, they are specifically excluded from the tools needed to defend themselves.

This legal gap is dangerous and must be addressed. While many critical infrastructure sectors face drone threats, correctional facilities present a uniquely high-risk environment. Prisons and jails cannot simply evacuate when an incoming drone is spotted. Our staff and those in our custody are on-site 24/7, with no option to pause operations. When drones breach the perimeter, correctional agencies cannot afford to wait for federal authorities to respond. We need lawful authority and tools to act immediately.

This gap in authority is untenable. The legal restrictions imposed on state and local corrections must be lifted if we are serious about securing our facilities and protecting our communities. On behalf of the American Correctional Association, I urge Congress to act now to extend tailored counter-UAS authorities to state, local, and especially correctional agencies.

The federal government has previously recommended pilot programs that would allow state and local governments to implement counter-UAS technologies under federal oversight. During the last Congress the House Transportation and Infrastructure Committee advanced legislation to do just that. And importantly, it included correctional institutions as eligible sites. We appreciate that recognition and view it as a meaningful step forward.

However, pilot programs alone are not enough. The threat we are facing is not limited to a few jurisdictions. It is widespread, organized, and escalating rapidly across the country. Hundreds of facilities across the country are seeing daily attempts to deliver dangerous contraband by drone. Limiting counter-UAS capabilities to a small number of pilot sites while the rest of the system remains unprotected is a temporary solution to a permanent and growing threat.

Congress must go further than pilot projects. Lawmakers must establish a legal framework that provides broad-based, but carefully regulated authority for correctional agencies - in addition to other state and local entities - to deploy and operate counter-UAS systems. This framework must be supported by funding, training, oversight, and transparency. It must be scalable and actionable across the entire correctional system, not just in isolated test locations.

Any legislation must explicitly include correctional facilities as part of the national counter-UAS strategy; provide resources to acquire drone detection and mitigation tools; ensure comprehensive staff training on UAS threats and response protocols; and establish oversight mechanisms to safeguard civil liberties and lawful drone use.

Every drone that breaches a prison fence is a direct threat to public safety. Each drone-triggered lockdown halts rehabilitation efforts and disrupts daily operations. And every day without action adds pressure to a correctional workforce already operating under extreme strain.

We are confronting 21st-century threats with outdated tools and without the legal authority to respond. That must change.

On behalf of the American Correctional Association and the corrections professionals we represent, I urge you to act swiftly to empower our institutions with the lawful tools, training, and support they need. We stand ready to assist in advancing a balanced, bipartisan solution.

U.S. Senate Committee on the Judiciary

Defending Against Drones:
Setting Safeguards for Counter Unmanned Aircraft Systems Authorities
May 20, 2025

Testimony of Professor Laura K. Donohue, J.D. Ph.D. (Cantab.)

Unmanned aerial systems (UAS) have become ubiquitous. They are employed for commercial delivery, journalism, agriculture, construction, surveying, law enforcement, firefighting, photography, sports broadcasting, film production, real estate sales, entertainment, and myriad other purposes.[1] They can be outfitted with technologies that extend well beyond ordinary audio or video collection to include RGB imagery, 4K and 8K video, near infrared, multispectral imaging, thermal infrared and light detection and ranging (LiDAR).[2] Functionally, UAS can be used to identify safety concerns, perform inspections, provide security, secure investments, and augment reality.[3] They also can be employed as a matter of artistic expression, as the FC Dallas Drone Show demonstrated so vividly in 2024, recreating classical pieces of art in the skies above Texas.[4] Reflecting their broad integration into daily life, the FAA has now registered more than one million drones, with approximately 421,000 commercial drone registrations and another 383,000 for recreational fliers.[5]

While UAS present numerous opportunities for work and leisure, they also can be levied by states and non-state actors for nefarious purposes. Even as the costs of commercial drones has plummeted, GPS-enabled flight and autonomous swarms present unique challenges.[6] They are accompanied by an expansion in payload capabilities. Drones can carry guns, bombs, flamethrowers, incendiary devices, and biological, chemical, or nuclear materials. They can be outfitted with tracking technologies, enhanced by physiological and behavioral biometric identification systems, to allow them to follow particular vehicles, individuals or groups of people.[7] They can integrate magnification to enable operators to read documents and to photograph or record sensitive information from significant distances. They also can deliver contraband. In 2020, for instance, a Department of Justice audit of the Federal Bureau of Prisons reported eighty-three incidents between 2015–2020 in which drones had been used to try to provide illicit materials to inmates.[8] Not only was the number of such deliveries annually increasing, but as the technology advanced, the amount

---

[1] *See, e.g.*, *Aerial Imaging Market Size, Share & Industry Analysis, By End Use (Real Estate & Architecture, Agriculture, Insurance, Environmental & Conservation (Urban Planning), Commercial & Advertising, and Others)*, FORTUNE BUSINESS INSIGHTS: AEROSPACE & DEFENSE, May 2025, https://www.fortunebusinessinsights.com/unmanned-systems-industry.
[2] *See* Jennifer Trock et al., *The Use of Unmanned Aircraft Systems in the Construction Industry in the United States and Canada*, 12 J. AM. COLL. CONSTR. LAWYERS 4 (2018).
[3] *Id.*
[4] *See* Sky Elements Drone Shows, Priceless Artwork Recreated using 500 Drones, FC Dallas Drone show, https://www.youtube.com/watch?v=I1whdYXNz3A.
[5] Federal Aviation Administration, *Drones by the Numbers (as of 4/1/2025)*, https://www.faa.gov/uas (last visited May 16, 2025) (noting "[r]ecreational flyers may use one registration number on multiple drones").
[6] *See generally* Jake Dulligan et al., *The Rising Threat of Non-state Actor Commercial Drone Use: Emerging Capabilities and Threats*, 18(3) COMBATING TERRORISM CENTER SENTINEL, Mar. 2025, https://ctc.westpoint.edu/the-rising-threat-of-non-state-actor-commercial-drone-use-emerging-capabilities-and-threats/; *see also* Ulrike Franke, *Drones in Ukraine and Beyond: Everything You Need to Know*, EUROPEAN COUNCIL ON FOREIGN RELATIONS, Aug. 11, 2023; Joshua A. Schwartz, *What Iran's Drone Attack Portends for the Future of Warfare*, MODERN WAR INSTITUTE, WEST POINT, Apr. 30, 2024; U.S. GOV'T ACCOUNTABILITY OFF., GAO-23-106930, SCIENCE & TECH SPOTLIGHT: DRONE SWARM TECHNOLOGIES (2023).
[7] *See generally* Laura K. Donohue, *Biomanipulation*, 113 GEO. L. J. 475, 505–29 (2025) (discussing PBCs and BBCs and the quality of information that can be remotely obtained).
[8] *See* DEP'T OF JUSTICE: OFF. OF THE INSPECTOR GEN., AUDIT OF THE DEPARTMENT OF JUSTICE'S EFFORT TO PROTECT FEDERAL BUREAU OF PRISONS FACILITIES AGAINST THREATS POSED BY UNMANNED AIRCRAFT SYSTEMS, 20-104, at 4 (2020), https://oig.justice.gov/sites/default/files/reports/20-104.pdf.

of material each UAS could carry expanding: in once instance, a single drone had been used to transfer twenty mobile phones, twenty-three phials of injectable drugs, dozens of syringes, and multiple packages of tobacco.[9] The weaponization of drones, their use in tracking and surveillance, and their role in providing illicit materials can be used to exploit vulnerabilities and undermine U.S. national security.

To address these and other threats, in 2018, Congress temporarily authorized the Department of Justice (DOJ) and Department of Homeland Security (DHS), without any prior consent, "to detect, identify, monitor, and track" any unmanned aerial system, to mitigate a credible threat posed by the aircraft "to the safety or security of a covered facility or asset."[10] The statute empowers the departments to warn operators and to disrupt control of the aircraft by disabling, intercepting, or interfering with wire, oral, electronic, or radio communications used to control the aircraft, to seize or confiscate the device, and, if necessary, to use reasonable force to damage or destroy it.[11] Continued intermittently, the provisions are set to expire September 30, 2025.[12]

Similar authorities have been extended to the military to "detect, identify, monitor, and track" and "disrupt control of," "seize or otherwise confiscate" or "use reasonable force to disable, damage, or destroy" drones threatening certain "facilities or assets."[13] The provisions are tied to particular locations, rendering it currently unlawful to operate personal drones within a 400-foot radius of military sites. Congress provided parallel powers to the Secretary of Energy in regard to certain nuclear facilities.[14] Unauthorized UAS sightings near military installations have continued, however, prompting Glen VanHerck, former joint commander of North American Aerospace Defense Command and U.S. Northern Command to suggest in March 2025 that there may be a foreign threat nexus.[15] His words echoed those of his successor, Gen. Gregory Guillot, who testified to the Senate Armed Services Committee in February 2025 about the need for more authorities.[16]

While the current statutory provisions and calls for expanded powers seek to address real threats which require attention, as written, the current statutory provisions already raise a number of constitutional concerns, amongst which are potential First and Fourth Amendment violations, as well as a violation of state sovereignty as protected by the Tenth Amendment. Ongoing appeals for expanded state powers,

---

[9] *Id.* at 2.
[10] Homeland Security Act of 2002, Pub. L. No. 107-296, tit. II, § 210G, as added by the FAA Reauthorization Act of 2018, Pub. L. No. 115-254, div. H, § 1602(a), 132 Stat. 3522 (Oct. 5, 2018).
[11] *See* FAA Reauthorization Act of 2018, Pub. L. No. 115-254, div. H, § 1602(a), Oct. 5, 2018, 132 Stat. 3522 (codified at 6 U.S.C. § 124n(b)(1)(B)–(F)).
[12] Set to expire "on the date that is 4 years after the date of enactment of this section" (i.e., Sept. 30, 2023). On September 30, 2023, Congress extended the provisions to November 18, 2023. *See* Continuing Appropriations Act, 2024, and other Extensions Act, Pub. L. No. 118-15, Sept. 30, 2023, 137 Stat. 71, § 2221. In November 2023, Congress extended the authorities to February 3, 2024. *See* Further Continuing Appropriations and Other Extensions Act, 2024, Pub. L. No. 118-22, div. B, tit. III, § 601, Nov. 17, 2023, 137 Stat. 123. In January 2024, Congress moved the expiration date to Mar. 9, 2024. *See* Pub. L. 118-35, Div. B, Title III, § 301, Jan. 19, 2024, 138 Stat. 7. On the day before the provisions were set to expire, March 8, 2024, Congress pushed the date out to May 11, 2024, at which point the legislature again moved the date to October 1, 2024. *See* Airport and Airway Extension Act of 2024, Pub. L. No. 118-41, tit. III, § 301, Mar. 8, 2024, 138 Stat. 24; FAA Reauthorization Act of 2024, Pub. L. No. 118-63, Title XI, §1112, May 16, 2024. (The latter statute also included a range of measures to integrate UAS into the national airspace.) In September 2024, Congress moved the date to December 20, 2024. *See* Continuing Appropriations and Extensions Act, 2025, Pub. L. No. 118-83, div. B, tit. I, § 101, Sept. 26, 2024, 138 Stat. 1534. In December 2024, the legislature shifted the date to March 14, 2025. *See* American Relief Act, 2025, Pub. L. No. 118-158, div. E, § 5102, Dec. 21, 2024, 138 Stat. 1771. And in March 2025, the new date was set for Sept. 30, 2025. *See* Full-year Continuing Appropriations and Extensions Act, 2025, Pub. L. No. 119-4, div. C, § 3102, Mar. 15, 2025, 139 Stat. 46.
[13] *See* 10 U.S.C. § 130i.
[14] *See* 50 U.S.C. § 2661.
[15] *See* Bill Whitaker, *How the U.S. is Confronting the Threat posed by Drones Swarming Sensitive National Security Sites*, CBS NEWS: 60 MINUTES (Mar. 16, 2025), https://www.cbsnews.com/news/drone-swarms-national-security-60-minutes-transcript/.
[16] *See Defense Officials Testify on 2026 Defense Budget Request*, C-SPAN (Feb. 13, 2025), https://www.c-span.org/program/senate-committee/defense-officials-testify-on-2026-defense-budget-request/655737.

moreover, overlook the significant range of authorities that have already been introduced to ensure that state and local authorities can respond to threats to critical infrastructure, correctional facilities, and large scale events. Whatever actions Congress decides to take to address the current state of UAS, such steps should be carefully construed to ensure constitutional consistency and respect for state rights.

I. First Amendment Considerations

The First Amendment reads,

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.[17]

Courts have long considered the act of audio and video recording to fall within the First Amendment's guarantee of speech and press rights.[18] The logic behind this approach is that it would be somewhat contrary to the established rights to say that speech and press were protected while simultaneously depriving an individual of the right to obtain the material to be conveyed (such as via drone).[19] As a matter of jurisprudence, the right to obtain footage includes the right to record law enforcement as well as government employees in the execution of their duties, within certain parameters.[20] The ability to do so undergirds one of the primary aims of the First Amendment, which is "to hold government officials accountable."[21] Like all constitutional entitlements, the right is not absolute: it can, for instance, be limited to performance of public duties in public spaces and be subjected to reasonable time, place, and manner restrictions.[22] Simultaneously, the right does not extend greater protections to the press than, for instance, to ordinary citizens.[23]

The UAS provisions which we are today discussing, together with DOJ's guidelines implementing the measures, implicate the First Amendment's protection of speech and assembly facially and as applied. They raise the spectre of the chilling effect doctrine, and they give rise to concerns related to the both the right to assemble as well as the right to petition the Government.

A. Facial Challenges to 6 U.S.C. § 124n

A law cannot be upheld merely because it is facially content- or speech-neutral. Intermediate scrutiny applies. In particular, a content-neutral law that implicates speech interests will be sustained if "it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest."[24] To meet this requirement, the regulation in

---

[17] U.S. Const amend. I.
[18] *See, e.g.*, ACLU of Ill. v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2014) ("The act of making an audio or audiovisual recording is necessarily included within the First Amendment's guarantee of speech and press rights as a corollary of the right to disseminate the resulting recording."); People for the Ethical Treatment of Animals, Inc. v. N.C. Farm Bureau Fed'n, Inc., 60 F.4th 815, 824–34 (4th Cir. 2023).
[19] *See, e.g.*, *Alvarez*, 679 F.3d at 595 (writing "the right to publish or broadcast an audio or audiovisual recording would be insecure, or largely ineffective, if the antecedent act of making the recording is wholly unprotected").
[20] *See, e.g.*, Turner v. Lieutenant Driver, 848 F.3d 678, 690 (5th Cir. 2017).
[21] *Id.* at 699.
[22] *See, e.g.*, Glik v. Cunniffe, 655 F.3d 78, 82–83 (1st Cir. 2011); *Turner*, 848 F.3d at 699.
[23] *See* Branzburg v. Hayes, 408 U.S. 665, 684 (1972) (writing, "the First Amendment does not guarantee the press a constitutional right of special access to information not available to the public generally."); *see also* Davis v. E. Baton Rouge Par. Sch. Bd., 78 F.3d 920, 928 (5th Cir. 1996) ("[T]he news media have no right to discover information that is not available to the public generally.").
[24] *United States v. O'Brien*, 391 U.S. 367, 377 (1968).

question does not have to be the least speech-restrictive means of advancing the governmental interest (as it does in the case of strict scrutiny). Instead, the narrow tailoring can be satisfied "so long as the . . . regulation promotes a substantial government interest that would be achieved less effectively absent the regulation."[25] In other words, it cannot " burden substantially more speech than is necessary to further the government's legitimate interests."[26]

Federal courts have upheld intermediate scrutiny as an appropriate level of review for facial challenges to UAS laws. In *National Press Photographers Association v. McCraw*, for example, the Fifth Circuit determined that although Texas state measures governing the operation of UAS in Texas airspace did not facially violate the First Amendment, they gave rise to concerns which warranted heightened scrutiny.[27] The Texas statute includes surveillance and no fly provisions, both considerably more detailed than the federal measures we are considering today.

The Texas surveillance provision makes it illegal to use a drone to "capture an image" of an individual or private property with the aim of surveilling the subject.[28] There are nearly two dozen exemptions to the rule, such as for academic research and military or law enforcement purposes.[29] Critically, for First Amendment purposes (and unlike the federal measures being addressed in the hearing today), these exceptions also make it lawful to capture images of public property or individuals on public property, or where the individual consents.[30] Texas law does not explicitly exempt media.

The Texas no fly provisions make it illegal to fly UAS up to 400 feet above certain critical infrastructure facilities, which include, *inter alia*, airports, power generators, and military installations, as long as they are enclosed by a fence or barrier, or there is some other indication that entry is forbidden.[31] Similar restrictions apply to correctional facilities and detention centers.[32] The law prohibits flight above large sports venues, including arenas, automobile racetracks, coliseums, stadiums, and other facilities which have the ability to hold 30,000 or more people.[33] The statute exempts government or law enforcement, the owner or operator of the venue, and anyone operating under license from the FAA or contract with the owner/operator of the venue.[34]

In 2020, Texan journalists, along with the Texas Press Association, brought a pre-enforcement challenge, seeking to enjoin the government from enforcing either the surveillance or no-fly provisions.[35] The Fifth Circuit determined in relation to the latter that while the First Amendment covers activities which are "inherently expressive," operation of a drone alone is not, continuing, "nor is it expressive to fly a drone 400 feet over a prison, sports venue, or critical infrastructure facility."[36] The statute merely conveyed flight restrictions.[37]

---

[25] United States v. Albertini, 472 U.S. 675, 689 (1985); *see also* Ward v. Rock Against Racism, 491 U.S. 781, 799 (1989).
[26] *Rock Against Racism*, 491 U.S. at 799. *See also* Reed v. Town of Gilbert, 576 U.S. 155, 174 (2015) (Alito, J., concurring) (noting "Time, place, and manner restrictions 'must be narrowly tailored to serve the government's legitimate, content-neutral interests.' But they need not meet the high standard imposed on viewpoint and content-based restrictions." (internal citations omitted)).
[27] *See* Nat'l Press Photographers Assoc. v. McCraw, 90 F.4th 770, 777 (5th Cir. 2024).
[28] *See* TEX. GOV'T CODE ANN. § 423.003(a) (West, Westlaw through 2025 Reg. Sess. 89th Leg.) (writing "A person commits an offense if the person uses an unmanned aircraft to capture an image of an individual or privately owned real property in this state with the intent to conduct surveillance on the individual or property captured in the image.").
[29] *See id.* §§ 423.002(a)(1), (3), and (8).
[30] *See id.*§ 423.002(a)(6) and (15).
[31] *See id.*§ 423.0045(a)(1-a), (b).
[32] *See id.* § 38.115(b).
[33] *See id.* § 423.0046(a), (b).
[34] *See id.* § 423.0046(c).
[35] *Id.* at 780.
[36] *Id.* at 787.
[37] *Id.* at 787–88.

The surveillance provisions proved more problematic. Courts have long considered restrictions on filming as triggering First Amendment concerns. "[T]he extent of constitutional protections for the right to film," the court noted, "is subject to ongoing and vigorous debate."[38] The court applied intermediate scrutiny on the grounds that the recording was not content based: i.e., individuals could obtain the same footage in other ways, such as by "using a helicopter, a tall ladder, a high building, or even a really big trampoline."[39] The fact that some individuals were exempted (e.g., academics, military personnel, and law enforcement) and not others (e.g., media), said nothing about the images themselves that were to be obtained.

The application of the same intermediate scrutiny test to the federal drone provision yields troubling results. The substantial government interests at issue include U.S. national security, the protection of critical infrastructure, and the safety and security of individuals and property.[40] But there are serious tailoring problems that attend. With more than one million drones operating in the United States, it would be fair to say that most drone operators harbor no ill intent towards U.S. national security or the safety and security of domestic individuals or property. Nevertheless, the provisions provide for the government, with no notice to any drone operators, to disrupt control of UAS by disabling the system and interfering in its command and control systems, seizing the device, confiscating it, or using force to disable, damage, or destroy the UAS.[41] There is *no* restriction in terms of the distance from the covered facility or asset, whether the UAS is travelling towards (or away) from such facility or asset, or whether it is located over private property. There is *no* discussion of what the drone is actually doing, what it may be observing, who may be operating the drone, or how many drones can be targeted in such manner. There is *nothing* to distinguish drones collecting information about public versus private spaces, with the result that all media coverage of any public activity can be prevented. It essentially allows the government to target all drones flying in the United States, even when located above private property, far from any critical facilities or assets, and flying well below the national airspace.

The current language fails intermediate scrutiny under the First Amendment. It burdens substantially more speech than is necessary to protect critical infrastructure, even as it potentially exempts any public or private facilities or conveyances designated by DOJ or DHS from scrutiny. Such constitutional deficiencies can result in troubling circumstances, significantly undermining First Amendment protections

In 2014, for instance, following Michael Brown's death in Ferguson, Missouri, law enforcement requested and obtained permission from the FAA to erect a no-fly zone over 37 square miles of airspace, making it impossible to obtain aerial footage of the protests that followed.[42] Following Freedom of Information Act requests, the Associated Press subsequently learned that the point of the prohibition was to prevent the media from recording the unrest.[43] U.S. Justice Department, reviewing more than 35,000 pages of police records and undertaking hundreds of interviews, found that the Fergusson Police Department had a pattern

---

[38] *Id.* at 788.
[39] *Id.* at 791.
[40] *See, e.g.*, 6 U.S.C. § 124n (k)(8) (including within the required risk-based assessment "an evaluation of threat information specific to a covered facility or asset and, with respect to potential impacts on the safety and efficiency of the national airspace system and the needs of law enforcement and national security at each covered facility"); *id.* at (k)(8)(G) (requiring as a factor for consideration the "[p]otential consequences to national security, public safety, or law enforcement if threats posed by the. Unmanned aircraft systems are not mitigated or defeated")
[41] 6 U.S.C. § 124n (b)(1)(C)–(F).
[42] *See* Camila Domonoske, *AP: No-Fly Zone in Ferguson Meant to Keep Media Out*, NPR NEWS, Nov. 2, 2014, https://www.wbur.org/npr/360991500/ap-no-fly-zone-in-ferguson-meant-to-keep-media-out. *See also* Russell Brandom, *Ferguson's No-fly Zone Was About Keeping the Media Out, According to New Documents*, Associated Press, posted on THE VERGE, Nov. 3, 2014, https://www.theverge.com/2014/11/3/7149445/fergusons-drone-blackout-was-about-keeping-the-media-out-faa.
[43] *Id.*

of interfering with the right to free expression in violation of the First Amendment as well as rights protected by the Fourth Amendment—matters of great public interest.[44]

The absence of any tailoring in 6 U.S.C. § 124n raises the possibility of precisely the types of abuses which the First Amendment was designed to prevent—abuses which have already occurred in relation to efforts to stop media from covering matters of tremendous importance to the electorate.

B. Content-based as Applied

As recognized by scholars, even if a statute is content-neutral on its face, "laws that are content-based as applied should be presumptively unconstitutional, just as facially content-based laws are presumptively unconstitutional."[45] In *Reed v. Town of Gilbert*, the Supreme Court explained,

> Government regulation of speech is content based if a law applies to particular speech because of the topic discussed or the idea or message expressed. . . . Our precedents have also recognized a separate and additional category of laws that, though facially content neutral, will be considered content-based regulations of speech: laws that cannot be "'justified without reference to the content of the regulated speech,'" or that were adopted by the government "because of disagreement with the message [the speech] conveys," Those laws, like those that are content based on their face, must also satisfy strict scrutiny.[46]

While the presumption may be rebutted (e.g., if speech falls within an exception or passes strict scrutiny), "generally speaking, when a law punishes speech because its content may cause harmful effects, that law should be treated as content based."[47] Just because a provision is generally applicable does not mean that it can evade serious First Amendment examination.[48]

The strict scrutiny standard demands that courts start from a presumption of unconstitutionality whereupon the government must demonstrate that the actions in question are narrowly tailored to further a compelling government interest, and that they constitute the least restrictive means possible to further that interest. While national security presents one of the most compelling interests held by the federal government, the drone provisions as applied do not come anywhere near meeting the strict scrutiny standard. Nor do they even satisfy the weaker intermediate scrutiny standard.[49]

The primary limitations on the statute's application focus on establishing *which* facilities are covered and requiring that the provisions be invoked "to mitigate a credible threat" as defined by the Secretary of DHS or the Attorney General.[50] Accordingly, the Attorney General has issued guidelines, which define "credible threat" as,

---

[44] *See* U.S. Department of Justice, Press Release: Justice Department Announces Findings of Two Civil Rights Investigations in Ferguson Missouri, Mar. 4, 2015, https://www.justice.gov/archives/opa/pr/justice-department-announces-findings-two-civil-rights-investigations-ferguson-missouri.

[45] Eugene Volokh, *Speech as Conduct: Generally Applicable Laws, Illegal Courses of Conduct, "Situation-Altering Utterances," and the Uncharted Zones*, 90 CORNELL L. REV. 1277, 1287 (2005).

[46] 576 U.S. at 163–64 (2015) (cleaned up).

[47] Volokh, *supra* note 45, at 41.

[48] On its face, 6 USC § 124n appears to be speech neutral, in that it applies to the conduct of drone flight, and not necessarily to the flight itself as a manifestation of speech. It also appears to be facially press-neutral in that it applies equally to private or public actors, regardless of their profession or purpose. They are thus considered generally applicable provisions. *See generally* Volokh, *supra* note 45, at 1294.

[49] *See supra* Section I.A.

[50] 6 U.S.C. § 124n (a).

> [T]he reasonable belief, based on the totality of the circumstances, that the activity of an unmanned aircraft or unmanned aircraft system may, if unabated:
>
> 1. Cause physical harm to a person;
> 2. Damage property, assets, facilities, or systems;
> 3. Interfere with the mission of a covered facility or asset, including its movement, security, or protection;
> 4. Facilitate or constitute unlawful activity;
> 5. Interfere with the preparation or execution of an authorized government activity, including the authorized movement of persons;
> 6. Result in unauthorized surveillance or reconnaissance; or
> 7. Result in unauthorized access to, or disclosure of, classified, sensitive, or otherwise lawfully protected information.[51]

The disjunctive "or" following the penultimate condition means that *any one of these* would be sufficient to meet the credible threat determination.

The first problem with this definition as grounds for designating facilities or assets is that, looking at the top of the list, *all* drones have the potential to "cause physical harm to a person." They do not need a particularly nefarious payload to do so. Rather, they need only fly into someone or even into an object, such as a plate glass window, to cause injury. Even drones weighing less than half a pound can be used, for instance, to blind someone. For anyone who has operated UAS, the danger to others and to property, the second condition listed above, is *precisely* why such objects are generally operated outdoors and away from crowded areas. Neither condition, however, is tied in any way to a covered facility or asset. The mere fact *that* a drone can do these things is sufficient. The definition similarly fails to connect the fourth condition, facilitating or constituting unlawful activity, to any particular facility or asset. Nor does the fifth bear any nexus: *any* interference in preparation or execution of a government activity counts, which encompasses picketing, protests, and other ways of conveying disapproval of officials' actions. Again, it does not have to in any way be linked to a particular facility or asset. It is not at all clear, additionally, what "unauthorized" means in the sixth and seventh conditions—nor does the surveillance have to be tied to the facility. And no definition is provided of what constitutes "sensitive" information.

Numerous government entities can make such requests. The Attorney General has authorized the Heads of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Agency (DEA), the Federal Bureau of Investigation (FBI), the Federal Bureau of Prisons (BOP), the United States Marshals Service (USMS), the Justice Management Division (JMD), and the Executive Office for United States Attorneys (EOUSA) to exercise counter-drone activities to identify facilities or assets considered a "high risk and potential target" for drone activity for approval by the Deputy Attorney General.[52] The government itself does not need to own or operate the facility. Instead, it merely must be located in the United States. Facilities, moreover, are broadly understood to include conveyances (such as vehicles transporting court witnesses) as well as law enforcement activities, emergency response, and security functions.

To satisfy the statutory requirement that the facility or asset be connected to one of the Department's authorized missions, the guidelines include, *inter alia*, any "National Special Security Event" (NSSE),

---

[51] William Barr, Attorney Gen., *Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems* (April 13, 2020), X(D), https://www.justice.gov/archives/ag/page/file/1268401/dl?inline (emphasis added).

[52] *Id.* at II(B). Note that any significant changes to previously designated covered facilities or assets, such as a change in the location, an expansion of the area, the deployment of a new protective measure) must be resubmitted. In an emergency, the department head can authorize the designation, with paperwork submitted to the Deputy Attorney General within five business days. *Id.* III(A)(4).

"Special Event Assessment Rating Event," or the provision of support to state, local, and territorial law enforcement for "mass gatherings."[53]

Remarkably, the very definition of NSSEs invokes heightened First Amendment protections because they are content-based: i.e., the guidelines define it in part as "a designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity."[54] To make this determination, the government *has* to look at the content of the speech itself, triggering strict scrutiny. Its application, though, fails to meet the standard to be applied. Far from being content-neutral, it is content-specific in a way that brings the government actions in regard to NSSE firmly within the meaning of the First Amendment. An additional point bears notice: terrorism is always a possibility. It is a method employed to any number of ends. Criminal activity, too, can occur any time, with the result that *all* political, economic, social, or religious events would fall within the statutory remit.

The "protective measures" which can be taken include "intercepting or otherwise accessing a wire, oral, or electronic communication used to control" the UAS or exercising control over the UAS—ostensibly including by intercepting any audio or video feeds.[55] *Any* drone feeds provided by UAS coverage can, for instance, be observed and seized by the government under the statutory provisions. These are incredibly broad methods that are overinclusive in relation to the purpose behind the provisions. These methods can be used against any drone, without any insight into whether the drone actually poses a terrorism or criminal threat. This is not the type of narrow tailoring that is constitutionally acceptable.

The definition of Special Event Assessment Rating (SEAR) Event allows for even broader application. The contours are set by a Federal Special Events Working Group chaired by DHS and FBI, with different levels of risk (on a scale of one to five) assigned to each.[56] They could include even small, local gatherings, such as parades or school board meetings.

The parallel risk assessment, which might otherwise limit the measures as applied, is required to note, amongst other conditions,

> [t]he potential consequences to national security, public safety, or law enforcement if threats posed by unmanned aircraft or unmanned aircraft systems are not mitigated or defeated, including any cybersecurity, espionage, intelligence, surveillance, reconnaissance, operational interference, criminal, chemical, biological, radiological, nuclear, or explosive-related risks.[57]

This understanding, however, applies everywhere and highlights further over-inclusivity problems: any drone carrying CBNRW would be considered of high consequence, regardless of where it was deployed within the United States. And any drone carrying CBNRW could threaten any facility or asset. Merely stating this is sufficient for any entity to be covered.

The upshot is that once approved, the facility or asset becomes a covered facility or asset at which protective measures can be deployed—without *any* particularity required as to specific drones subsequently observed, controlled, seized, or destroyed.[58] This is wildly overinclusive.

---

[53] *Id.* at III(C)(4).
[54] *Id.* at X(F).
[55] *Id.* at X(G).
[56] *See id.* at X(H); Off. Of Operations Coordination, Dep't of Homeland Sec., *Fact Sheet: What are Special Event Assessment Rating (SEAR) Events?*, https://www.dhs.gov/sites/default/files/publications/19_0905_ops_sear-fact-sheet.pdf.
[57] *See* Barr, *supra* note 51, at III(F)(3)(g).
[58] *Id.* at III(K)(1), (3).

The Guidelines go on to note that components "may only intercept, acquire, access, maintain, use, or disseminate communications in a manner consistent with the Constitution, including the First and Fourth Amendments."[59] Similar to the provisions in the Foreign Intelligence Surveillance Act,

> A component may not deploy or use any protective measure under authority of the Act solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of rights secured by the Constitution or laws of the United States. A component should consider and be sensitive at all times to the potential impact protective measures may have on legitimate activity by unmanned aircraft and unmanned aircraft systems, including systems operated by the press.[60]

The problem with the sole purpose provision is that the facilities have already been designated, bypassing the restriction that the activity be undertaken "solely for the purpose of monitoring" First Amendment activities.

As applied to journalism, the Supreme Court has noted that "generally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news."[61] In the case of Texas, where surveillance provisions protected only private individuals and property, the Fifth Circuit determined that the press had "no special privilege to invade the rights and liberties of others."[62] But a key distinction in the case was that the provisions related to private—not public—property. In fact, the statute explicitly allowed drones to be used to obtain images on "public real property or a person on that property."[63] The federal provision makes no such distinction.

C. Interplay of 6 U.S.C. § 124n with the Chilling Effect Doctrine

The drone provisions risk having a chilling effect on media coverage of government activities, as well as matters of great political, religious, economic, and social importance. The doctrine stems from the Cold War, in the context of loyalty oaths.[64] Continued efforts throughout the 1950s and 60s provided the courts with numerous opportunities to consider their impact.[65] By 1967, in Justice Harlan's words, the "chilling effect" doctrine had become "ubiquitous."[66]

---

[59] *Id.* at IV(A).
[60] *Id.* at VI(A).
[61] Cohen v. Cowles Media Co., 501 U.S. 662, 669 (1991).
[62] *Nat'l Press Photographers Assoc.*, 90 F.4th at 793 (internal quotation omitted).
[63] *Id.* (quoting § 423.002(a)(15)).
[64] *See* Wieman v. Updegraff, 344 U.S. 183 (1952).
[65] *See, e.g.*, Keyishian v. Board of Regents, 385 U.S. 589 (1967) (holding New York statute making treasonable or seditious words or acts grounds for removal from state employment and barring anyone willfully advocating or teaching he forcible overthrow of government as unconstitutionally vague and a violation of the First Amendment); Lamont v. Postmaster Gen., 381 U.S. 301 (1965) (holding unconstitutional a statute requiring the post office to detain and destroy unsealed mail from foreign countries determined to be communist political propaganda absent the addressee submitting a reply card indicating their desire to receive such mail); Baggett v. Bullitt, 377 U.S. 360 (1964) (holding Washington state statutes requiring teachers and state employees to take oaths unconstitutionally vague); Gibson v. Florida Legis. Investigation Comm., 372 U.S. 539, 556–57 (1963) (holding that state legislative committee directed to investigate subversive and Communist activities had failed to demonstrate a substantial connection between a race relations group and Communist activities and could not be compelled to product membership records); Shelton v. Tucker, 364 U.S. 479, 486 (1960) (holding as unconstitutional a statute compelling teachers as a condition of employment to annually file an affidavit listing all organizations to which they have belonged or regularly contributed over the previous five years); Sweezy v. New Hampshire, 354 U.S. 234, 246–50 (1957) (holding contempt conviction for a professor's refusal to answer questions about his lectures and knowledge of a political party to be a violation of the First Amendment).
[66] Zwickler v. Koota, 389 U.S. 241, 256 n.2 (1967) (Harlan, J., concurring).

The concept of deterrence resides at the heart of the doctrine: individuals in some sense may be restrained from undertaking certain speech or actions, or being associated with others or groups, with whom they otherwise might be in communion. The reason may be because of a fear of reprisal or punishment: fines, imprisonment, civil liability, or social or economic consequences. The question is whether an individual is inhibited from participating in activity that is protected, regardless of whether it is free exercise of religion, free speech, freedom of the press, or the right to assemble. Fear, risk, and uncertainty are part of the calculus as to what comparative harm an individual would suffer if he or she engaged in such expression.

By 1971, the composition of the Court had shifted, prompting a shift in the doctrine. In *Laird v. Tatum*, the Supreme Court drew a limit, holding that "Allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[67] *Laird*, a case brought by anti-war protesters, focused on intelligence collection in the midst of civil disorder. Following the assassination of Dr. Martin Luther King, President Lyndon B. Johnson had ordered the military to assist civilian authorities in Detroit, Michigan.[68] The U.S. Army had subsequently collected information at public meetings, forwarding it back to Army Intelligence headquarters at Fort Holabird, Maryland, and then disseminating the information to Army posts across the United States.[69] Approximately 1,000 agents had been engaged in the operation.[70] The Court noted that while the litigants argued that the information amassed could be misused, they neither claimed that it was foreseeable, nor grounded their complaint in the concern. Instead, they solely argued that it created an impermissible burden on their ability to fully utilize their First Amendment rights.[71] The mere existence of intelligence gathering, however, was not sufficient grounds on which to find a chilling effect.[72]

In his dissent, Justice Douglas, joined by Marshall, protested, "[i]f Congress has passed a law authorizing the armed services to establish surveillance over the civilian population, a most serious constitutional problem would be presented."[73] The Founders' fears of a standing army existed not just "in bold acts of usurpation of power, but also in gradual encroachments."[74] For Douglas, "The authority to provide rules 'governing' the Armed Services means the grant of authority to the Armed Services to govern themselves, not the authority to govern civilians."[75] Such military "power must be carefully limited lest the delicate balance between freedom and order be upset."[76] Douglas explained, "The act of turning the military loose on civilians even if sanctioned by an Act of Congress, which it has not been, would raise serious and profound constitutional questions. Standing as it does only on brute power and Pentagon policy, it must be repudiated as a usurpation dangerous to the civil liberties on which free men are dependent."[77] He concluded, "The 'deterrent effect' on First Amendment rights by government oversight marks an

---

[67] *See* Laird v. Tatum, 408 U.S. 1, 13–14 (1972).
[68] *Id.* at 4–5.
[69] *Id.* at 6.
[70] *Id.* at 7.
[71] *Id.* at 9–10.
[72] *Id.* at 10.
[73] 408 U.S. at 16 (Douglas, J., dissenting).
[74] *Id.* at 18.
[75] *Id.* at 18–19.
[76] *Id.* at 19.
[77] *Id.* at 24; *see also id.* at 24–25 ("It is alleged that the Army maintains files on the membership, ideology, programs, and practices of virtually every activist political group in the country. . . . The Army uses undercover agents to infiltrate these civilian groups and to reach into confidential files of students and other groups. The Army moves as a secret group among civilian audiences, using cameras and electronic ears for surveillance. The data it collects are distributed. . . . [T]he charge is that the purpose and effect of the system of surveillance is to harass and intimidate the respondents and to deter them from exercising their rights of political expression, protest, and dissent 'by invading their privacy, damaging their reputations, adversely affecting their employment and their opportunities for employment, and in other ways.' [. . .] Judge Wilkey, speaking for the Court of Appeals, properly inferred that this Army surveillance 'exercises a present inhibiting effect on their full expression and utilization of their First Amendment rights.'")

unconstitutional intrusion."[78] While standing acted for a number of years as a barrier to First Amendment chilling claims, as intelligence collection has expanded, (as heralded in the current drone context, in regard to the type and extent of information collected, or the potential number of people implicated), numerous cases alleging a chilling effect have met the standing requirement.[79]

In the matters before this committee today, all it might take would be the interruption of one flight, either by the government assuming control, by seizing the UAS, or by destroying it, to chill the likelihood of others collecting footage. We have already seen instances in which the federal government had enacted measures to prevent the media, for instance, in reporting on certain conditions.

In October 2021, for instance, the FAA implemented a two week Temporary Flight Restriction over international bridge in Del Rio, Texas, with the result that Fox News could no longer provide footage of, and information about, some 8,000 people who had been congregating on the Texas-Mexico border.[80] Concerns immediately emerged that instead of addressing the border crisis, the Biden Administration was trying to cover it up.[81] Although later lifted, giving the government the authority to capture any footage picked up by drones in the vicinity may well chill others' willingness to engage in critique of the Administration's decisions.

The chilling effect becomes particularly problematic in light of the regulatory guidelines which target drone flights above religious, political, economic, or social functions—even if held on private property.[82] The Supreme Court has held that any effort by the government to compel membership lists in certain organizations, for instance, may violate freedom of association under the First Amendment.[83] In *NAACP v. Alabama ex rel. Patterson*, the Court held that requiring the NAACP to disclose its group membership would likely have an adverse impact on members' ability "to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and the consequences of this exposure."[84] It mattered naught that "whatever repressive effect compulsory disclosure" may have stemmed from private community pressure: "The crucial factor is the interplay of governmental and private action, for it is only after the initial exertion of state power represented by the production order that a private action takes hold."[85]

D. Impact on the Right to Petition

A final consideration worth mentioning relates to the right to petition, an entitlement often overlooked, but one which, at least at the Founding, was considered far more important than the speech and associative rights most commonly associated with the First Amendment.[86] It was, in part, because the new U.S.

---

[78] *Id.* at 25 (quoting *Lamont*, 381 U.S. at 307).
[79] *See, e.g.*, Am. C.L. Union v. Clapper, 785 F.3d 787 (2d Cir.2015); Schuchardt v. President of the United States, 839 F.3d 336, 341–50 (3d Cir. 2016); Wikimedia Found. v. Nat'l Sec. Agency, 857 F.3d 193 (4th Cir. 2017).
[80] *See* Andrew Mark Miller & Bill Melugin, *Fox News Cleared to Fly After Biden FAA Temporarily Bans Drones Over Bridge Packed With Illegal Immigrants*, FOX NEWS (Sept. 17, 2021, 1:59 PM), https://www.foxnews.com/politics/bidens-faa-places-temporary-ban-on-drones-flying-over-bridge-packed-with-illegal-immigrants.
[81] *See* Samuel Chamberlain, *FAA Grounds Fox News Drones Near Where Thousands of Migrants Are Sheltering Under a Bridge*, N.Y. POST (Sept. 17, 2021), https://nypost.com/2021/09/17/faa-grounds-fox-news-drones-in-texas-near-sheltering-migrants/ (running Fox News footage after the Administration lifted the prohibition).
[82] *See* Barr, *supra* note 51, at X(F).
[83] See NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 462 (1958).
[84] *Id.* at 462-3.
[85] *Id.* at 463.
[86] *See* JOHN PHILLIP REID, CONSTITUTIONAL HISTORY OF THE AMERICAN REVOLUTION: THE AUTHORITY OF RIGHTS 4 (1986); Julie M. Spanbauer, *The First Amendment Right to Petition Government for a Redress of Grievances: Cut from a Different Cloth*, 21 HASTINGS CONST. L.Q. 15, 17, 34–39 (1993); Norman B. Smith, *"Shall Make No Law Abridging . . . ": An Analysis of the Neglected, But Nearly Absolute, Right of Petition*, 54 U. CIN. L. REV. 1153, 1165–67 (1986); *see also* Laura K. Donohue, *The*

Constitution had failed to protect the right that Anti-Federalists roundly attacked the new framework.[87] The right was considered so important that while the prefatory clauses in the First Amendment single out Congress, the petition clause extends to all three branches of government, attaching as much to the executive and judicial branches as to the legislative one.[88] The reason was simple: the right protects active, political engagement. It prevents limiting citizens' interaction to the ballot box, instead empowering a continuous conversation between the government and the governed. It ensures that officials cannot insulate themselves, or limit access just to those who are more favored. It establishes an expectation that officials will respond to requests. And it provides a steam valve to diffuse tension.

In 1978, the Supreme Court recognized that this clause plays a critical "role in affording the public access to discussion, debate, and the dissemination of information and ideas."[89] It goes beyond concepts like freedom of the press or individual self-expression "to prohibit government from limiting the stock of information from which members of the public may draw."[90] The public has a right to get information about the government. This right of access extends to obtaining information from, and about "all departments of the Government."[91]

Like all rights, the right of petition and its concomitant right of access is not absolute. In *Press Enterprise Co. v. Superior Ct.*, the Supreme Court articulated a two-part test for the First Amendment right to public access: "First, because a 'tradition of accessibility implies the favorable judgment of experience,' we have considered whether the place and process have historically been open to the press and general public."[92] The Court continued, "Second, in this setting the Court has traditionally considered whether public access plays a significant positive role in the functioning of the particular process in question."[93] The Court continued, "If the particular proceeding in question passes these tests of experience and logic, a qualified First Amendment right of public access attaches."[94]

This inquiry, referred to as the "experience and logic" test, is used to determine whether or not access must be granted to certain areas or facilities. While both elements must be met for the right of access to attach, the first takes precedence.[95] Resultantly, "[i]t is only where access has traditionally not been granted that we look to logic. If logic favors disclosure in such circumstances, it is necessarily dispositive."[96]

The statutory provisions related to designating certain facilities and assets as covered by the drone regulations, which can then be used to prevent the public from any access to events which occur on or near such facilities (or, indeed anywhere), fail to account for the importance of the experience and logic test in ascertaining whether the government even has a right to prohibit the public from observing certain areas and obtaining information. They impermissibly leave all such designations to DOJ and DHS, without any discussion of whether the government even has the constitutional authority to close such facilities to inspection.

Common Law and First Amendment Qualified Right of Public Access to Foreign Intelligence Law, 112 GEO. L. J. 271, 298–301 (2024).

[87] *See, e.g.*, Centinel II, PHILA. FREEMAN'S J. (Oct. 24, 1787), reprinted in 13 THE DOCUMENTARY HISTORY OF THE RATIFICATION OF THE CONSTITUTION 457, 466–67 (John P. Kaminski et al., eds., 1981); Richard Henry Lee's Amendments, 27 September, reprinted in 13 THE DOCUMENTARY HISTORY OF THE RATIFICATION OF THE CONSTITUTION, *supra*, at 238, 239.

[88] *See* Donohue, *supra* note 86, at 299.

[89] First Nat'l Bank of Bos. v. Bellotti, 435 U.S. 765, 783 (1978).

[90] *Id.*

[91] Cal. Motor Transp. Co. v. Trucking Unlimited, 404 U.S. 508, 510 (1972).

[92] Press Enterprise Co. v. Superior Ct., 478 U.S. 1, 8 (1986) (citation omitted) (quoting *Globe Newspaper Co.*, 457 U.S. at 605).

[93] *Id.*

[94] *Id.*

[95] As the Ninth Circuit has explained, "Where access has traditionally been granted to the public without serious adverse consequences, logic necessarily follows." In re Copley Press, Inc., 518 F.3d 1022, 1026 & n.2 (9th Cir. 2008).

[96] *Id.* at 1026 n.2.

II. Fourth Amendment

The Fourth Amendment states,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[97]

The current statutory provisions raise Fourth Amendment concerns in relation to general warrants, with concerns about geofencing providing a parallel analysis. The countermeasures appear to constitute both a search and a seizure, moreover, for which a particularized warrant is required. The provisions run rampant over property rights and the Fourth Amendment's protection of "effects", and could under some circumstances give rise to concerns about the collection of geolocational data. Analogies can be drawn to cell site simulators, for which particularized warrants are generally required. Under Supreme Court doctrine, simply asserting that the threat is of great interest to domestic security does not excuse the government from the warrant requirement.

A. General Warrant

The Founding generation adopted the Fourth Amendment in response to significant concerns in the wake of the Constitutional Convention that the common law prohibition against general warrants, and the need for particularized warrants, be retained as a way to offset the expansion in federal power. A general warrant is a document issued by an official or member of the judiciary, not based on any prior evidence of wrongdoing. It lacks particularity regarding the person or place to be searched, or the papers or records to be seized. Unsupported by any oath or affirmation, it is used to find evidence of criminal activity. At the Founding, it was well recognized that such muniments violated the "reason of the common law" and thus were considered an "unreasonable" search or seizure (thus the inclusion of "unreasonable searches and seizures" in the Fourth Amendment).[98] The second part of the clause goes on to spell out exactly what constitutes sufficient particularities for a particularized warrant to be valid: probable cause, an oath or affirmation of wrongdoing, and a description of the place to be search and persons or things to be seized.

One of the most glaring concerns in the current statutory language which governs UAS search and seizure is that it essentially operates as a general warrant. It gives the federal government the authority to intercept or access all communications between the drone operator and the UAS used to control it, as well as to disrupt and seize control of all UAS systems.[99]

The statute ties its understanding of wire, oral, and electronic communications to criminal law provisions. Specifically, a "wire communication" is "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce."[100] The government also can intercept "any oral communication uttered by a person exhibiting an expectation

---

[97] U.S. Const. amend IV.
[98] *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 UNIV. CHICAGO L. REV. 1181 (2016).
[99] 6 U.S.C. § 124n(b)(1)(A), (C),(D).
[100] 18 U.S.C. § 2510 (1).

that such communication is not subject to interception."[101] Electronic communication, in turn, "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce."[102]

The meaning of UAS is similarly tied to provisions in the U.S. code which broadly define it as "an unmanned aircraft *and associated elements* (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system."[103]

The upshot of the statute's reliance on these definitions is that the government can seize not just communications directing the drone where to fly, but also communications related to what the drone itself is collecting, observing, and communicating back to the drone operator.

It also means that the government gains access to any devices used over the course of such transmissions, whether it be radio frequency signals, Wi-Fi, or satellites, which play a critical role in communicating with drones (particularly for devices flown beyond visual line of sight (BVLOS)). Even common commercial drones, such as those sold by DJI, a prominent Chinese drone maker, rely on satellite technologies. They use Global Navigation Satellite System (GNSS) receivers for accurate georeferencing and positioning, as well as features like DJI AirSense which employ Automatic Dependent Surveillance-Broadcast (ADS-B) technology for situational awareness and collision alerts.[104] They also offer Real-time Kinematics (RTK) and Post-Processing Kinematics (PPK) for commercial and industrial applications requiring high-precision positioning.[105] The former supplies real-time correction data from a base station, while the latter provides a backup system, where raw satellite data can be processed later. These capabilities are included in even starter-level drones like the Phantom 4 RTK.[106] Various other applications, such as DJI's photogrammetry (i.e., the science of extracting reliable information about physical objects and the environment by capturing and analyzing electromagnetic radiation—essentially generating 3D models or maps from aerial images), rely on satellite positioning for accurate georeferencing and mapping.

There is nothing in the statutory provisions to limit government access to such satellites, or to ground stations with which they communicate. Search and seizure of such devices does not need to be tied to any sort of probable cause. Instead, at the say so of local operators, the government can simply engage in a search of such devices to try to find evidence of wrongdoing. The provisions thus act as a general warrant.

Various drone mitigation technologies can be employed, with varying implications. The government, for instance, may use RF sensors, which passively monitor radio frequencies used by drones for communications or listen for characteristic radio signals (e.g., 2.4 GHz and 5.89 GHz bands). Alternatively, optical cameras can be used to identify and track drones. They can be integrated with other technologies such as radar or acoustic sensors (more effective than RF for instance, if the flight pattern has been pre-programmed), to provide a multi-sensor approach. Once that occurs, various mitigation and

---

[101] 18 U.S.C. § 2510 (2).
[102] 18 U.S.C. § 2510 (12).
[103] 49 U.S.C. § 44801 (12) (emphasis added).
[104] *See generally* Run Li, *Unlocking Aerial Mapping and Data Collection: Elevate Your Operations with the Power and Precision of DJI's LiDAR Technology*, Mastering LiDAR with DJI Enterprise: An Introductory Booklet (Jan. 18, 2024), https://enterprise-insights.dji.com/blog/lidar-basic-guide#:~:text=GNSS%20(Global%20Navigation%20Satellite%20System,sensor%20during%20the%20data%20capture; DJI AirSense, https://www.dji.com/flysafe/airsense#:~:text=DJI%20AirSense%20is%20an%20alert,airwaves%20by%20adding%20additional%20transmissions.
[105] *See generally* RTK Hardware, DJI Enterprise, https://enterprise-insights.dji.com/blog/rtk-real-time-kinematics.
[106] *Id.*

countermeasures may be employed, such as jamming, which interferes with RF, disabling drone communication and control. Spoofing can create false GPS signals to divert the drone or interrupt its navigation. Operators, alternatively, could simply take remote control of the drone, or it could use various kinetic options to intercept, disable, or destroy the drone. But none of these steps can be taken until the drone is identified, as it may be by constant scans of certain areas.

In this sense, the detection systems employed may share similarities with geofencing, in which GPS or RFID technology is used to create a virtual geographic boundary enabling software to trigger a response when a mobile device enters or leaves a particular area. Geofence warrants allow law enforcement to compel companies, like Google, to provide location data from their users' devices within a particular location during a specific timeframe. Vendors then provide a list of mobile phones present within the window requested. Such warrants, which have become more widespread over the past ten years, tend to be used when law enforcement knows the approximate location of criminal activity, but not the identity of the person themselves.[107] Like the drone provisions, they lack particularity.[108] They also raise significant privacy concerns because they can collect data from a large number of people, and not just from individuals suspected of wrongdoing.[109]

Unlike the drone provisions, however, geofence warrants involve a third party magistrate, demonstration of probable cause, and an oath or affirmation. Even so, the Circuits are split as to whether such warrants still constitute general warrants and thus violate the Fourth Amendment.[110] Just last year, for instance, the Fifth Circuit held that geofence warrants constitute general warrants and are presumptively unconstitutional.[111] As explained above, 6 U.S.C. § 124n suffers from the same constitutional defect with the notable addition of not having any warrant procedures in place.

When courts have assessed geofence warrants to determine whether or not they should be granted, moreover, they have analyzed whether the government's application is supported by probable cause and whether it is sufficiently particularized.[112] Probable cause requires a showing that "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[113]

6 U.S.C. § 124n does not apply just to criminal activity; nor does it require a showing that meets the probable cause requirement. A "reasonable ground to believe" in the totality of the circumstances[114] is not the same as a "fair probability." In an application denying a geofence warrant a district court explain that "the particularity requirement for a geofence warrant is satisfied if [it] narrowly identifies the place to be searched by time and location so that it is not overbroad in scope."[115] The fact that a proposed geofence boundary would encompass "two public streets" that may have lots of people on it during the relevant time that might have nothing to do with criminal activity was a problem.[116] As aforementioned, the 6 U.S.C. § 124n application has no restriction on how close it needs to be to the actual covered facility or asset, other

---

[107] United States v. Smith, 110 F.4th 817, 821 (5th Cir. 2024)
[108] *Id.* at 821.
[109] *See generally*, Jake Laperruque, *Geofence Warrants: The Last Piece of the Location Privacy Puzzle*, Project on Gov't Oversight, Aug. 25, 2021, https://www.pogo.org/analysis/geofence-warrants-the-last-piece-of-the-location-privacy-puzzle#:~:text=And%20then%20there%20are%20geofence,the%20same%20risks%20as%20stingrays.
[110] *Smith*, 110 F.4th at 817; United States v. Chatrie, 2025 WL 1242063 (4th Cir. Apr. 30, 2025); United *States v. Davis*, 109 F.4th 1320 (11th Cir. 2024).
[111] *Smith*, 110 F.4th at 838.
[112] *See Matter of Search of Info. that is Stored at Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1158–59 (D. Kan. 2021); *United States v. Easterday*, 712 F. Supp. 3d 46, 51-53 (D.D.C. 2024).
[113] *Illinois v. Gates*, 462 U.S. 213, 214 (1983)
[114] *See* Barr, *supra* note 51, at III(f), X(d,
[115] 542 F. Supp. 3d at 1158.
[116] *Id.*

than the general "necessary to mitigate" language in the statute. This raises the same particularity problems which dog geofence warrants, as would the lack of time restrictions.

B. The Warrant Requirement

6 U.S.C. § 124n explicitly authorizes the government to conduct a search and seizure of UAS, bringing such actions within the meaning of the Fourth Amendment in at least three ways: first, the ancient doctrine of *ad coelem* raises the spectre of trespass in government examination and expropriation of drones located above public and privately-owned property; second, UAS, including the component parts directing flight such as ground stations and satellites, constitute "effects"; and third, under *United States v. Carpenter*, the locational data collected by the government in searching UAS, if persistent, may be subject to constitutional protections.

1. Property Rights: Ad Coelum

Legal doctrine clearly establishes that property rights convey control over adjacent airspace, with interference considered a trespass or nuisance, depending upon the context. The statutory provisions allowing the government to search and seize drones located over either private or state-held property amount to an unconstitutional interference in the airspace above the land.

As Franciscus Accurius wrote in *Glossa Ordinaria* (1220-1250 CE), a work which for 500 years provided the authoritative statement of Justinian law, "*Cuius est solum, eius est usque ad coelum et ad inferos*" (*Trans*. "Whoever owns land it is theirs up to the heavens and down to hell."). For more than a millennium the concept of *ad coelum* has treated terrestrial rights, and the landowner's entitlement to the air above, as coextensive.[117] The Justinian concept quickly worked its way into English Common Law, with Sir Edward Coke writing in his *First Institute of the Laws of England*, "And lastly the hearth hath in law a great extent upward, not only of water as hath been said, but of aire, and all other things even up to heaven, for *cujus est solum ejus est usque ad coelum*, as it is holden."[118]

Blackstone later explained the rights conveyed in real property: "Land hath also, in its legal signification, an indefinite extent, upwards as well as downwards. *Cuius est solum, eius est usque ad coelum*, is the maxim of the law, upwards; therefore no man may erect any building, or the like, to overhang another's land: and, downwards, whatever is in a direct line between the surface of any land, and the center of the earth, belongs to the owner of the surface."[119]

Consistent with this doctrine, throughout the 17th and 18th centuries English courts recognized that trespass on airspace violated landowners rights.[120] Even passing over another's property in an air balloon constituted a violation. The American colonies and later, states, incorporated *ad coelum* into domestic law, with the result that by the nineteenth century, state courts routinely considered even overhanging branches to constitute a trespass as well as a nuisance.[121] Even when the invasion was temporary and did no actual damage, it still violated the property owner's rights.[122]

---

[117] *See* Laura K. Donohue, *Who Owns the Skies? Ad Coelum, Property Rights, and State Sovereignty*, in EYES TO THE SKY: PRIVACY AND COMMERCE IN THE AGE OF THE DRONE (Matthew Feeney ed., Cato Institute (2021).
[118] Edward Coke, "Of Real Property, and First or Corporeal Hereditaments of Land," The First Part of the Institutes of the Lawes of England (London: Rawlins, Roycroft, and Sawbridge, 1684). *See also* Donohue, *supra* note 117.
[119] William Blackstone, Commentaries on the Laws of England, vol. 2 (London, G.W. Childs., 1866), p. 18.
[120] *See* Donohue, *supra* note 117.
[121] *See, e.g.*, Grandone v. Lovdal, 70 Cal. 161, 11 P. 623 (1886); Tanner v. Wallbrun, 77 Mo. App. 262 (1898); Countryman v. Lighthill, 24 Hun. (N.Y.) 405 (1881).
[122] *See, e.g.*, Herrin v. Sutherland, 74 Mont. 587, 241 P. 328 (1925) (holding that shooting a duck flying over another person's property constitutes trespass).

The Supreme Court followed suit, finding in *Portsmouth Harbor Land & Hotel Company* that the routine discharge of a battery amounted to a taking.[123] Justice Holmes, writing for the Court, noted,

> If the United States, with the admitted intent to fire across the claimants' land at will, should fire a single shot or put a fire control upon the land, it well might be that the taking of a right would be complete. But even when the intent thus to make use of the claimants' property is not admitted, while a single act may not be enough, a continuance of them in sufficient number and for a sufficient time may prove it. Every successive trespass adds to the force of the evidence.[124]

In 1946, the Supreme Court held in *United States v. Causby* that anything below navigable airspace was in the control of the landowner: "The superadjacent airspace at [a] low altitude is so close to the land that continuous invasions of it affect the use of the surface of the land itself. We think that the landowner, as an incident to his ownership, has a claim to it and that invasions of it are in the same category as invasions of the surface."[125]

Although the federal government followed *Causby* by re-defining "navigable airspace" to include "airspace needed to insure safety in take-off and landing of aircraft," the Supreme Court again recognized that landowners controlled the airspace over their property, writing in the 1962 case of *Griggs v. Alleghany*, "[T]he use of land presupposes the use of some of the airspace above it. Otherwise, no home could be built, no tree planted, no fence constructed, no chimney erected. An invasion of the superadjacent airspace will often affect the use of the surface of the land itself."[126]

6 U.S.C. § 124n does not acknowledge landowners' rights. To invade such rights on any sort of ongoing basis (such as in continual scans of communications sent to or from drones above private property, or the interception of transmissions or exertion of control over the same), the government would have to first obtain a warrant. The statute, however, as aforementioned, does nothing of the sort. Instead, as outlined by the Attorney General guidelines, when an authorized agency would like to make use of the law, it merely submits a written request to the Deputy Attorney General to confirm which facility or asset are covered and what protective measures will be deployed.[127] This application must, among other things, explain why there is a reasonable ground to believe, in the totality of the circumstances, that the activities of UAS represent a credible threat to the safety and security of the facility or asset.[128] There is no hard limit on the length of time such measures may be in place. Nor, as explained above, is there any geographic limitation on how far these measures extend in relation to a covered facility or asset other than the general statutory limitation that the authorized methods may be approved for what is "necessary to mitigate a credible threat."[129] They are put in place once approved by the Deputy Attorney General and are, presumably, to be employed against *any* UAS without regard to what the UAS is actually doing, who is controlling it, what its purpose is, and other similar considerations.

In contrast to the federal provisions, numerous states in their drone laws have continued to recognize landowners' rights in the airspace above their property. Nevada state law, for instances, states, "The ownership of the space above the lands and waters of this state is declared to be vested in the several owners

---

[123] Portsmouth Harbor Land & Hotel Co. v. United States, 260 U.S. 327 (1922).
[124] 260 U.S. at 329–30.
[125] United States v. Causby, 328 U.S. 256, 265 (1946).
[126] Griggs v. Alleghany, 369 U.S. 84, 85 (1962).
[127] *See* Barr, *supra* note 51, at III.
[128] *Id.* at III(F).
[129] 6 U.S.C. 124n(a).

of the surface beneath."[130] Consistent with this understanding, Nevada state law empowers landowners to bring an action for trespass against the operator of an unmanned aerial vehicle (UAV) flown at a height of less than 250 feet, subject to a handful of exceptions.[131] North Carolina similarly prohibits anyone from conducting UAS surveillance of a person or dwelling or private real property without the owner's consent.[132] South Dakota prohibits trespass on property using a drone with the intent to subject anyone to surveillance.[133] Tennessee makes it a misdemeanor to use a drone "to capture an image of an individual or privately owned real property in Tennessee with the intent to conduct surveillance on the individual or property captured in the image."[134] California prohibits entering a landowner's airspace to capture any image of individual's engaging in private, personal, or familial activity without permission.[135]

Numerous states, moreover, require that state and local law enforcement, outside exigent circumstances, obtain a warrant prior to using drones for certain activities and forbid use of UAV to establish either reasonable suspicion or probable cause.[136] Tennessee's "Freedom from Unwarranted Surveillance Act", for instance, states "The use of a drone . . . by a law enforcement agency to search for and collect evidence or obtain information or other data shall constitute a search" unless authorized by a warrant.[137] Utah state law reads, "A law enforcement agency or officer may not obtain, receive, or use data acquired through an unmanned aircraft system unless the data is obtained [] pursuant to a search warrant."[138] States also limit the amount of time for which a warrant operate.[139]

It is quite remarkable to see a complete absence of any equivalent protections at a federal level. And while the federal provision allows for retention of information for 180 days, for most states, information obtained with a prior warrant can only be kept for 15 or fewer days, unless it is to be used as evidence in criminal prosecution.[140] State provisions are often supplemented by numerous municipal ordinances.[141]

To the extent that state-owned and operated drones are being flown over state-owned land, any federal interference would fall subject to the same restrictions which accompany private landowners' rights. Numerous states, again, recognize state sovereignty and control of such airspace.[142] (*See* Part III, below).

2. UAS as "Effects"

---

[130] NEV. REV. STAT. ANN. § 493.040 (West, Westlaw through 83rd Reg. Sess. (2025).
[131] *Id.* at 493.103.
[132] NC GEN. STAT. ANN. § 15A-300.1(b) (West, Westlaw through 2024 Reg. Sess.).
[133] S.D. CODIFIED LAWS § 22-21-1 (West, Westlaw through the 2025 Reg. Sess.).
[134] TENN. CODE ANN. § 39-13-903 (West, Westlaw through 2025 First Reg. Sess.).
[135] A.B. 856 (Cal. 2015).
[136] *See, e.g.*, NEV. REV. STAT. ANN. § 493.112 (West, Westlaw through 83rd Reg. Sess. (2025); NC GEN. STAT. ANN. § 15A-300.1(c)(3) (West, Westlaw through 2024 Reg. Sess.); OR. REV. STAT. § 837.310 (2024 Reg. Sess. 82nd Legis. Assem.); TENN. CODE ANN. § 39-13-609(e)(2) (West, Westlaw through 2025 First Reg. Sess.).;TEX. GOV'T CODE ANN § 423.001(West, Westlaw through 2025 Reg. Sess. 89th Leg.); UTAH CODE ANN. § 72-10-802 (West, Westlaw through 2025 General Sess.).
[137] TENN. CODE ANN. § 39-13-609 (West, Westlaw through 2025 First Reg. Sess.).
[138] UTAH CODE ANN. § 72-10-802(West, Westlaw through 2025 General Sess.) (containing certain exceptions).
[139] *See, e.g.*, NEV. REV. STAT. ANN. § 493.112 (West, Westlaw through 83rd Reg. Sess. (2025); (limiting it to 10 days); OR. REV. STAT. § 837.310 (2024 Reg. Sess. 82nd Legis. Assem.) (limiting it to 30 days).
[140] *See, e.g.*, TENN. CODE ANN. § 39-13-609 (West, Westlaw through 2025 First Reg. Sess.).
[141] In California, for instance, dozens of municipal ordinances restrict drone flight. See, e.g., Town of Los Alamitos Mun. Ord. 2018; City of Yorba Linda Mun. Ord. 2017; Town of Calabasas Mun. Ord. 2017; City of Hermosa Beach Ord. 16-1363 2016; Sacramento County Code 9.36.068 2018; San Francisco Park Code § 3.09 1981; Santa Clara Valley Open Space Authority Reg. § 11.01.01 2018; Mid Peninsula Regional Open Space District Lands Regs. § 409.4 2014; City of La Mesa Mun. Ord. 2005; City of Malibu Filming Permit; Mountains Recreation & Conservation Authority Park Ordinance 2018; City of Rancho Palos Verde Mun. Ord. 1991; City of Napa Mun. Code 12.36.130. Other states, however, have prohibited any governmental sub-units from introducing their own provisions.
[142] *See, e.g., id.* at 493.030.

In addition to "persons, houses, [and] papers", the Fourth Amendment protects "effects". As Professor Maureen Brady has argued, personal property in public space gives rise to significant privacy and security interests.[143] At the time of the Founding, the protection against unreasonable searches and seizures was intimately tied to laws prohibiting interference with possession of personal property, such as dispossession, damage, or unwanted handling.[144] But that is precisely what the federal drone provisions do: they give the government permission to undertake each of these interferences, without any warrant supported by probable cause.

To the extent that the government takes control of such effects, the sensor and collection capabilities of the drones may give rise to further concerns about what information is collected. The statutory provisions, however, deal only with how long information obtained may be kept—and nothing about what information, in the first place, can be obtained. Under the provisions, moreover, the government may disseminate any footage or communications obtained from a drone if, for instance, the information obtained revealed completely unrelated criminal activity, essentially hijacking personal devices.[145]

Take, for instance, a circumstance in which a farmer is surveying a pond adjacent to his home, some fifty miles from any covered facility. The government, under the statutory provisions could take control of the drone, direct it to the home, zoom in through the window, and acquire footage of the family inside. If any illegal activity is observed, that video can then be provided to local law enforcement for prosecution. In fact, the government can take over control of any drone anywhere in the United States and use it to obtain whatever footage it would like of events occurring on private property, without ever obtaining a warrant justifying search either of the effect itself, or of the persons or houses located in the vicinity.

3. Location data

6 U.S.C. § 124n allows for the government to collect location data without any limitation on the length of time such information is obtained. In 2017, though, the Supreme Court held in *Carpenter v. United States* that the warrantless search and seizure of cell phone records, including the location and movement of the users, violated the Fourth Amendment.[146]

A close analogue here may be the constitutional analysis related to cell-site simulators (also known as IMSI catchers): electronic surveillance devices which imitate a cell tower's signal and trick nearby phones into communicating with it. These devices enable law enforcement to obtain location and identifying information, as well as potentially other data such as calls, texts, and the contents of communications, from mobile phones in the vicinity. There are significant concerns about the privacy implications because they can be used to track individuals even inside their homes (where they have a heightened expectation of privacy), as well as to intercept users' communications. As a result of public outcry, DOJ guidelines now require federal agencies to obtain warrants before using IMSI catchers, outside of exigent circumstances.[147]

Concerns about the collection of location data and the consequent need for a warrant have already surfaced in the drone context. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, grassroots organizations challenged law enforcement's implementation of the Aerial Investigation Research (AIR)

---

[143] *See* Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 YALE L.J. 946 (2016).
[144] *Id.* at 981–994.
[145] *See* Barr, *supra* note 51, at VI(C)(2).
[146] Carpenter v. United States, 585 U.S. 296 (2018).
[147] *See* Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology, Sept. 3, 2015, p. 3 https://www.justice.gov/d9/press-releases/attachments/2015/09/03/doj_cell-site_simulator_policy_9-3-15.pdf (stating "prosecutors should. . . . either (1) obtain a warrant that contains all information required to be included in a pen register order pursuant to 18 U.S.C. 3123 (or the state equivalent), or (2) seek a warrant and pen register order concurrently.")

program, which recorded activity occurring within the city.[148] Consistent with *Carpenter*, the Fourth Circuit determined that because the program enabled the police to deduce from individuals' movements, access to the data constituted a search. The extent to which a similar argument could be levied in regard to 6 U.S.C. § 124n would depend upon the nature and extent of interference in UAS, limits to which are not provided by the statutory language.

4. Investigations Relating to Domestic Security Still Require a Warrant

One argument frequently raised in support of broader authorities for UAS relates to the severity of the threat: namely, that where national security is at risk, special procedures need to be adopted. While it is true that issues of domestic national security may not always require the same warrant procedures adopted in criminal law cases, the Supreme Court in *U.S. v. U.S. District Court* ("Keith") made it clear that measures to address domestic national security that implicate the Fourth Amendment require "prior judicial review."[149] Some sort of probable cause standard attaches. This, after all, was the impetus for Congress's introduction of the 1978 Foreign Intelligence Surveillance Act, which has repeatedly been upheld by the courts as constitutional.[150]

Here, however, 6 U.S.C. § 124n operations have nothing even approximating a warrant. They require only the approval of the Deputy Attorney general or, in emergencies, the head of an authorized agency.[151] This raises the very *nemo iudex in causa sua* problems that the Court deemed unconstitutional in *Keith*.

III. State Rights

In 2014 the Federal Aviation Administration (FAA) posted an article on its website entitled, Busting Myths about the FAA and Unmanned Aircraft. Exhibit #1 was the "myth" that "The FAA doesn't control airspace below 400 feet."[152] To the contrary, the agency claimed, "The FAA is responsible for the safety of U.S. airspace from the ground up."[153]

To some extent, the statement is accurate: the FAA is responsible for the safety of U.S. airspace. It simultaneously is misleading and wrong: while the FAA is constrained in what it can do in relation to UAS,

---

[148] Leaders of a Beautiful Struggle v. Baltimore Police Department, 2F.4th 330, 333 (4th Cir. 2021).
[149] United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 323–24 (1972) (Keith).
[150] *See, e.g.*, United States v. Nicholson, 955 F. Supp. 588, 590-91 (E.D. Va. 1997) (holding FISA as constitutional); United States v. Cavanagh, 807 F.2d 787, 790–92 (9th Cir. 1987) (per then-Circuit Judge Kennedy) (rejecting argument that FISA violates the Fourth Amendment and Article III); United States v. Duggan, 743 F.2d 59 (2d Cir.1984) (rejecting challenges to FISA under the Fourth and Fifth Amendments and under the Equal Protection Clause of the Fourteenth Amendment); United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982) (rejecting argument that FISA violates Fifth and Sixth Amendments); United States v. Spanjol, 720 F.Supp. 55, 58 (E.D. Pa. 1989) (rejecting challenge to FISA under the Fourth Amendment); United States v. Ott, 637 F.Supp. 62 (E.D.Cal.1986), aff'd, 827 F.2d 473 (9th Cir.1987) (rejecting challenge to FISA under the Due Process Clause); *In the Matter of Kevork*, 634 F.Supp. 1002 (C.D. Cal. 1985) (rejecting challenges to FISA under the Fourth Amendment and Article III); *United States v. Falvey*, 540 F.Supp. 1306 (E.D.N.Y. 1982) (rejecting challenges to FISA under the First, Fourth, Fifth, and Sixth Amendments); *see also* Ellsberg v. Mitchell, 709 F.2d 51, 66 n. 66 (D.C. Cir. 1983) (noting that FISA had theretofore survived all constitutional challenges), cert. denied, sub nom. Russo v. Mitchell, 465 U.S. 1038 (1984); United States v. Benkahla, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006) (holding FISA ELSUR and physical search procedures as consistent with the Fourth Amendment); United States v. Muhtorov, 187 F. Supp. 3d 1240, 1250, 1255 (D. Colo. 2015), aff'd, 20 F.4th 558 (10th Cir. 2021) (holding that the FISA-acquired evidence (under §702) should not be suppressed because its collection did not violate the Fourth Amendment, and, while the defendant does have a reasonable expectation of privacy in his communications it is "diminished when transmitted to a third party over the internet."); United States v. Warsame, 547 F. Supp. 2d 982, 993 (D. Minn. 2008) (holding that FISA's probable cause and particularity requirements satisfy the reasonableness requirement of the Fourth Amendment).
[151] Barr, *supra* note 51, at III(a).
[152] Busting Myths about the FAA and Unmanned Aircraft, reproduced at https://www.asprs.org/news-resources/busting-myths-about-the-faa-and-unmanned-aircraft.
[153] *Id.*

it has little to no claim to the air just above the ground. Instead, as aforementioned both private and public landowners own low-altitude airspace and air rights, with states in the primary position for enforcement.[154] The current way in which the regulations are written in regard to federal powers run rampant over both.

As explained in Professor Eugene McQuillin's *The Law of Municipal Corporations*,

> The public right to the use of streets goes to the full width of the street, and extends, indefinitely upward and downward. On the ground, therefore, of failure to exercise ordinary care to keep public ways in a reasonably safe condition for travel, municipal negligence may be established, on the theory of a defect in the street, in action for damages due to injuries to travelers from awnings, signs, billboards, poles, electric wires, or other objects suspended over, or near thereto, or falling into a street or sidewalk.[155]

It is to the states, and not to the federal government, that we look for ownership and control of property within each state which is not formally owned by the federal government.

Under the U.S. Constitution, states retained all powers neither delegated to the federal government nor prohibited to them.[156] The Tenth Amendment encompassed a range of authorities: under it, police powers (relating to health, welfare, and morals), criminal law, and corporate charters fell within the state domain. To states went authority for education, manufacturing, and agriculture. States bore the responsibility to regulate, control, and govern real and personal property, as well as individuals located within the state. As the Supreme Court noted in 1905,

> Although this court has refrained from any attempt to define the limits of [state police powers], yet it has distinctly recognized the authority of a state to enact quarantine laws and health laws of every description; indeed, all laws that relate to matters completely within its territory and which do not by their necessary operation affect the people of other states.[157]

The Court later suggested that "laws relating to matters completely within the territory of the state" belonged to the state itself.[158]

Control of real property, including the airspace above (outside of land owned outright by the federal government) falls within the purview of state and local government. As the Supreme Court acknowledged, "[A] State has the same undeniable and unlimited jurisdiction over all persons and things, within its territorial limits, as any foreign nation."[159] State authority "is complete, unqualified and exclusive."[160] Thus, while landowners' title to water may extend to the low-water mark, the ground beneath was held by the state, not the federal government. So, too, do states control and place any applicable restrictions on landowners in their use and enjoyment of property, such as building heights, permits, and the placement of fences.

---

[154] *See* Laura K. Donohue, A Tale of Two Sovereigns: Federal and State Use and Regulation of Unmanned Aircraft Systems, in HANDBOOK OF UNMANNED AERIAL VEHICLES (Kimon P. Valavanis & George J. Vachtsevanos eds., Springer International Publishing AG 2d ed.) (2015).
[155] Eugene McQuillin, A Treatise on the Law of Municipal Corporations, vol. 8 (Chicago: Callaghan and Co., 1921), § 2775 (internal quotations omitted); *see also* McQuillin, Municipal Corporations, vol. 6 (1913), § 2775; Incorporated Town v. Cent. States El. Co., 204 Iowa 1246, 1250, 214 N.W. 879, 54 A.L.R. 474 (1927) (quoting McQuillin).
[156] U.S. Const. amend. X.
[157] Jacobson v. Massachusetts, 197 U.S. 11, 25 (1905) (internal quotations omitted).
[158] Thomas Cusack Co. v. City of Chi., 242 U.S. 526, 531 (1917).
[159] New York v. Miln, 36 U.S. 102, 139 (1837).
[160] *Id.*

The advent of air travel initially had almost no impact on such rights. The Uniform Aeronautics Act, the first model statute to circulate, emphasized state sovereignty over airspace, landowners' rights above their property, and other provisions relating to aircraft.[161] Twenty-two states adopted it in some form.[162] As for whether overflight constituted a trespass, case law repeatedly considered the question to be well within the state domain. In *Smith v. New England Aircraft Co.*, for instance, the Supreme Court of Massachusetts wrote,

> It is essential to the safety of sovereign States that they possess jurisdiction to control the airspace above their territories. It seems to us to rest on the obvious practical necessity of self-protection. Every government completely sovereign in character must possess power to prevent from entering its confines those whom it determines to be undesirable. That power extends to the exclusion from the air of all hostile persons or demonstrations, and to the regulation of passage through the air of all persons in the interests of the public welfare and the safety of those on the face of the earth. This jurisdiction was vested in this Commonwealth when it became a sovereign State on its separation from Great Britain.[163]

When the Air Commerce Act of 1926 passed, it acknowledged dual sovereignty and the rights of state governments, distinguishing navigable airspace from that controlled by the states.[164] Only aircraft in the former could be controlled by the federal government. Initially, federal regulations established a floor of 1,000 feet over cities, towns, and settlements, and 500 feet over all other land, subject to certain exceptions.[165] Numerous states followed suit, prompting litigation over the status of *ad coelum*.

In *Swetland v. Curtiss Airports Corporation*, the Sixth Circuit noted that while "the law reports of practically every state" referred to the concept, the right was not absolute; nevertheless,

> [t]his does not mean that the owner of the surface has no right at all in the air space above his land. He has a dominant right of occupancy for purposes incident to his use and enjoyment of the surface, and there may be such a continuous and permanent use of the lower stratum which he may reasonably expect to use or occupy himself as to impose a servitude upon his use and enjoyment of the surface.[166]

The landowner could not "reasonably expect to occupy" the upper stratum. Here, the only right of the landowner was "to prevent the use of it by others to the extent of an unreasonable interference with his complete enjoyment of the surface."[167] While in the lower strata, interference might constitute a trespass, in the upper it might be merely a nuisance.

In the intervening years, the federal government has consistently made an effort to claim ever more control over state land.[168] The courts, however, have continued to acknowledge state rights. In *United States v. Causby*, the Supreme Court recognized that granting the federal government control over lower airspace would give them "complete dominion and control over the surface of the land."[169] One of the latest efforts to narrow state rights even further appeared in the FAA Reauthorization Act of 2018, which limited the

---

[161] *See* William A. Schnader, *Uniform Aviation Liability Act*, 9 J. AIR L. & COM. 9 664 (1938). For discussion of the evolution of the model statute, see George Gleason Bogert, *Recent Developments in the Law of Aeronautics*, 8 CORNELL L.Q. 26 (1923).
[162] *Id.*
[163] *See, e.g.*, Smith v. New England Aircraft Co. [Mass.] 170 N.E. 385 (1930).
[164] 44 Stat. 571, § 5(b).
[165] Air Commerce Regulations (Dec. 1926), Chapter 7, § 74(G)
[166] 55 F.2d at 203.
[167] *Id.*
[168] *See generally* Donohue, *supra* note 117.
[169] Causby, 328 U.S. at 262.

hobbyist carve-out to 400 feet above ground level.[170] In 2013, the Congressional Research Service acknowledged the tension between federal claims and individual and state rights.[171]

What perhaps makes these matters even more complicated is that *almost every state now has UAS regulations*, many of which already deal with concerns presented to this committee. Numerous states, for instance, make it illegal to fly UAS above or near prisons and critical infrastructure.[172] States have laws restricting UAS over open-air athletic facilities and large scale events.[173] States forbid the weaponization of unmanned vehicles.[174] States claim the right to control airspace within their borders. In Nevada, for

---

[170] *See* FAA Reauthorization Act of 2018, Pub. L. No. 115-254.

[171] *See* Alissa M. Dolan & Richard M. Thompson II, Cong. Research Serv., R42940, *Integration of Drones into Domestic Airspace: Selected Legal Issues* 2 (2013), https://fas.org/sgp/crs/natsec/R42940.pdf.

[172] *See, e.g.*, S.B. 1449,52nd Leg., 2d Reg. Sess.(Ariz. 2016), ARIZ. REV. STAT. ANN. 13-3729 (West, Westlaw through First Reg. Sess. Fifty-Seventh Legis. (2025) (prohibiting UAS flight within 500 feet horizontally or 250 feet vertically of any critical facility, including but not limited to federal, state, county, or municipal jails or prisons; oil and gas facilities; water treatment facilities; power plants, courthouses, military installations; and hospitals); ARK. CODE ANN. § 5-60-103 (West, Westlaw 2025 Reg. Sess. 95th General Assem.) (prohibiting flight over, *inter alia*, electrical power plants, petroleum refineries, railroads, communication towers, and correctional or detention facilities); CAL. PENAL CODE § 4577(a) (West, Westlaw through 2025 Reg.Sess.) (prohibiting UAS flight above a state prison, jail, juvenile hall, camp, or ranch); FLA. STAT. ANN. § 330.41 (West, Westlaw through 2025 first reg. sess.) (prohibiting operation of a drone over a critical infrastructure facility, allowing a drone to make contact with any person or object at such a facility, or coming close enough to interfere with the operations or to cause a disturbance to the facility, and defining such facilities as, inter alia, power generation, refineries, gas processing, airports, spaceports, military installations, dams, and both state-run and private correctional facilities); GA SB 6 (Act 67) (prohibiting use of UAS to deliver or attempt to deliver contraband to places of incarceration); Iowa HF 2492 (prohibiting use of UAS in, on, or above any municipal holding, detention, or correctional facility or the surrounding grounds subject to certain exceptions); Kentucky SB 157 (KY Acts c. 061) (prohibiting UAS over critical infrastructure, correctional facilities, and military installations); LA.. STAT. ANN. § 337 (West, Westlaw through 2024 First Extraordinary, Second Extraordinary, Reg., Third Extraordinary Sess.) (prohibiting use of UAS over critical infrastructure and correctional facilities); MN Stat. Sec. 243.552 (prohibiting UAS in airspace over state correctional facilities or grounds belonging to or land controlled by the facility without the written consent of the commissioner of corrections); NEV. REV. STAT. ANN. § 493.109 (West, Westlaw through 83rd Reg. Sess. (2025) (prohibiting UAV flight within 500 feet horizontally or 250 feet vertically from a critical facility, defined as power plants, water treatment facilities, pipelines, chemical or petroleum facilities); N.J. STAT. ANN. § 2C:40-28 (West, Westlaw through L.2025, c. 38 and J.R. No. 5) (prohibiting UAS flight over correctional facilities); N.C. GEN. STAT. ANN. § 15A-300.3 (West, Westlaw through 2024 Reg. Sess. General Assem.) (prohibiting UAS within 500 horizontal or 250 vertical feet over prisons); OK H.B. 2599 (prohibiting unmanned aircraft over critical infrastructure facilities less than 400 feet above the ground); Or. H.B. 4066 (prohibiting UAS over critical infrastructure facilities and correctional institutions less than 400 feet above the ground); Pa. Act 78 of 2018 (H.B. 1346), § 3505(a) (making it illegal to provide, transmit or furnish contraband); S.C. CODE ANN. § 24-1-300 (West, Westlaw through 2025 Act No. 2) (prohibiting UAV within 250 vertical feet of a correctional facility); SC § 24-5-175 (prohibiting UAV within 250 feet of a detention facility); S.D. CODIFIED LAWS § 50-15-3 ((West, Westlaw through the 2025 Reg. Sess.) (prohibiting drone flight over correctional, detention, and military facilities absent administrator consent); TENN. CODE ANN. § 39-13-903 (West, Westlaw through 2025 First Reg. Sess.) (prohibiting flight of unmanned aircraft over correctional facilities or within 250 feet of the perimeter of any critical infrastructure facility with the business operator's consent); TEX. GOV'T CODE ANN. § 423.0045 (West, Westlaw through 2025 Reg. Sess. 89th Leg.) (prohibiting flight of unmanned aircraft over critical infrastructure); stadiums); Utah § 14-1-304 (prohibiting operation of UAS "to carry or drop any item to or inside the property of a correctional facility" or to interfere with its operation); WIS. STAT. ANN. §114.045, 175.55 (West, Westlaw through 2025 Act 5) (prohibiting drone flight over the grounds of any state correctional institution without authorization).

[173] *See, e.g.*, DEL. CODE ANN. tit. 11, c. 5, § 1334 (West, Westlaw through ch. 16 153rd General Assem. (2025-2026)) (prohibiting UAS over any sporting event, concert, automobile race, festival, or other event at which more than 1,500 people are in attendance, over any critical infrastructure, or over any incident where first responders are actively engaged); Rev. Stat. of Missouri § 217.850 (prohibiting UAS over correctional facilities and "open-air facilities such as stadiums, sports venues, theaters, music venues, performing arts facilities, and entertainment facilities which can seat 5,000 or more people); TENN. CODE ANN. § 39-13-903 (West, Westlaw through 2025 First Reg. Sess.) (prohibiting use of unmanned aircraft to capture image of an individual or event at an open-air event venue wherein more than 100 individuals are gathered for a ticketed event, provided there is no consent from the venue owner or operator); TEX. GOV'T CODE ANN. § 423.0046 (West, Westlaw through 2025 Reg. Sess. 89th Leg.) (prohibiting unmanned aircraft over sports venues with a seating capacity of 30,000 or more people outside of certain conditions).

[174] *See, e.g.*, NEV. REV. STAT. ANN. § 493.106, 193.130 (West, Westlaw through 83rd Reg. Sess. (2025); NC GEN. STAT. ANN. § 14.401.24 (West, Westlaw through 2024 Reg. Sess.); OR. REV, STAT. § 837.365 (2024 Reg. Sess. 82nd Legis. Assem.); UTAH CODE ANN. § 72-10-902 (West, Westlaw through 2025 General Sess.); WIS. STAT. ANN. § 941.292 (West, Westlaw through 2025 Act 5).

instance, a provision relating to "Sovereignty in space" states: "Sovereignty in the space above the lands and waters of this state is declared to rest in the State, except where granted to and assumed by the United States pursuant to a constitutional grant from the people of the State."[175]

Unlike the federal statutes which form the basis for the hearing today, state law frequently acknowledges the right of owners to fly drones over their own property, as well as to exclude others from their airspace.[176] There is nothing, however, in the federal provisions which acknowledges state control over these areas, bringing them into direct conflict with the rights reserved to the states under the Tenth Amendment.

IV. Principles of Construction

There are numerous ways Congress could address the threat posed by UAS while still ensuring that the statutory provisions structurally and substantively meet constitutional requirements. The guiding principles should center on isolating specific facilities which present the greatest risk, requiring public notice and a nexus between the threat posed by a specific drone and proximity to the site, introducing a warrant procedure for the interception of communications, and exempting private and state-owned drones flown over non-federal land. A few examples of how this could be done follow.

First, Congress could redraw the statute to ensure that fewer facilities are covered and that only UAS actually threatening critical facilities are included (e.g., in terms of distance from the covered facility), thus helping to protect citizens' First Amendment activities. In 2017, when Congress first extended the authority to the military to respond to UAS, it did so in relation to specific mission sets: i.e., nuclear deterrence, missile defense, and national security space.[177] It simultaneously gave the Department of Energy the power to use counter UAS technology in relation to special nuclear material.[178] The following year, DOD obtained additional authorities, again tied to particular missions: protecting the President or Vice President, U.S. air defense, combat support agencies, special operation activities, and the production, storage, transportation, or de-commissioning of high-yield explosives.[179] It also included Major Range and Tast Facility Bases, as statutorily defined.[180]

In contrast, 6 U.S.C. § 124n allows for DHS to target UAS in regard to *any* "buildings, grounds, and property that are owned, occupied, or secured by the Federal Government."[181] The regulations further allow DHS and DOJ to target drones in relation to any NSSE or SEAR events, which, as aforementioned, are broadly written and include events of "political, economic, social, or religious significance", all of which are First Amendment protected activities.[182]

These definitions should be significantly narrowed and foreclosed in the statutory provisions, as should the definition of "covered facility". Right now, the agencies can name any building or area considered a high risk for UAS activity, instead of facilities which contain, for instance, sensitive nuclear materials. The emphasis is on whether a drone may fly overhead, not on what it is that is being protected. Yet myriad federal agencies have nothing to do with highly sensitive national security matters.

---

[175] NEV. REV. STAT. ANN. § 493.030 (West, Westlaw through 83rd Reg. Sess. (2025).
[176] *See, e.g.*, ARK. CODE ANN. § 5-60-103(c)(1) (West, Westlaw 2025 Reg. Sess. 95th General Assem.) (exempting surveillance over property owned, leased, or licensed as well as by third parties retained by the owners or insurance companies).
[177] National Defense Authorization Act, Pub. L. No. 114-328, §§ 1697, 3112, 130 Stat. 2000, 2639-40, 2756 (2017).
[178] *Id.* at §§ 1697, 3112.
[179] National Defense Authorization Act, Pub. L. No. 115-91, § 1692 (2018).
[180] *Id.*
[181] 40 U.S.C.A. § 1315(a). *See also* 6 U.S.C. § 124n(k)(3)(C)(I)(III) (stating "protection of facilities pursuant to section 1315(a) of Title 40).
[182] William Barr, Attorney Gen., *Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems* (April 13, 2020), X(F), https://www.justice.gov/archives/ag/page/file/1268401/dl?inline.

Many state measures, moreover, limit the flight of drones to a specific horizontal as well as vertical distance above certain facilities (e.g., 250 feet from a correctional facility). The federal measures do not. Instead, they simply say that the government can target drones (anywhere), in order to protect the critical facilities. Congress could address this by limiting the distance from which the drone is flying from the facility itself.

There is a distinction to be drawn between no fly and no surveillance measures, which the current statutory language conflates. While both implicate First Amendment concerns, it is the former that causes the greatest concern in terms of threat. In an age of satellite surveillance, it would be naïve to assume that the latter would prevent adversaries from being able to observe U.S. facilities, so it makes little sense to place such restrictions on the media and others within domestic bounds. Currently, however, there are no such protections, again in contrast to state statutes, which explicitly allow the capture of images of public property or individuals on public property, as well as where property owners consent.[183]

Simultaneously, as aforementioned, the Fourth Amendment protects U.S. citizens from persistent surveillance by the U.S. government. State provisions recognize this by prohibiting law enforcement use of drones without a warrant. There is no equivalent provision at a federal level to stop the government from routinely searching UAS or assuming control of the drones and using them to place private operators, located on private land, under surveillance. Introducing a warrant procedure, which is subject to an exigent circumstances exception, and restricting what can be done with the drone and which communications could be obtained could help to address this concern.

A warrant procedure also would go some way towards addressing Fifth Amendment due process concerns that could easily arise in situations in which forced landings occur and/or the government takes possession of the drone.[184] Under *Matthews v. Eldridge*, due process determinations require an examination of three distinct factors: "First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail."[185] Additional safeguards to prevent the government from being able to assume control of, and deprive an individual of their property would help to strengthen the constitutional sufficiency of the UAS provisions.

Finally, as currently written, 6 U.S.C. § 124n contains no explicit recognition of state rights. To the contrary, it claims control of drones in state airspace and would allow the federal government to assume control of state-owned drones as well. UAS located 400 feet or below fall within state, not federal, purview. So, too, does the state exercise control over its own UAS. It is only above federal land, or in the national airspace, that the federal government can control state-owned drones. This needs to be explicitly acknowledged in the federal provisions to ensure that DHS and DOJ do not overreach their constitutional limits.

V. Concluding Remarks

UAS offer tremendous commercial and creative opportunities. At the same time, they can be used in myriad ways that could endanger people and property, critical infrastructure, or U.S. national security. In addressing this threat, however, it is critical that Congress not overreach.

---

[183] *See, e.g.*, TEX. GOV'T CODE ANN. 423.002(a)(6) and (15).

[184] The due process clauses found in the Fifth and Fourteenth Amendments ensure that the government cannot deprive an individual of his or her property absent notice, an opportunity to be heard, and a determination by a neutral decisionmaker. See U.S. Const. amends V, XIV.

[185] Matthews v. Eldridge, 424 U.S. 319, 335 (1976).

The recent spate of drone sightings proves illustrative. They spurred panic and prompted the FAA to impose a slew of temporary flight restrictions: at least thirty in New York and another twenty-two in New Jersey.[186] The FAA announced that the government may use "deadly force" in the event that UAS posed an "imminent security threat".[187] It later emerged that a number of the sightings, even those near critical infrastructure, were simply normal air traffic.[188] Had the government responded aggressively to the sightings, human life could have been imperiled.

The incident, and the various examples noted above, serve as a strong reminder that while it is necessary to address real threats, there is a reason that the U.C. Constitution erects procedural and substantive protections. Whatever course Congress decides to pursue must comport with the protections of rights enshrined in the First and Fourth Amendments, as well as rights reserved to the states through the Tenth Amendment.

Thank you.

---

[186] FAA Imposes Flight Restrictions in NY Amid Drone Mayhem, NBC N.Y., Dec. 20, 2024, https://www.nbcnewyork.com/new-york/drone-update-news-faa-ban/6081619/.

[187] Ayesha Ali and Clara McMichael, *FAA Temporarily Bans Drones in Parts of New Jersey, New York adds flight restrictions*, ABC NEWS, Dec. 20, 2024, https://abcnews.go.com/US/drone-updates-faa-temporarily-bans-drone-operations-parts/story?id=116936091.

[188] *See* Matthew Petti, *Newly Released Documents Show What the Feds Knew About the New Jersey Drone Scare*, REASON, May 9, 2025, https://reason.com/2025/05/09/what-the-feds-knew-about-the-new-jersey-drone-scare/#:~:text=On%20December%2017%2C%202024%2C%20the,Goff%20wrote%20in%20an%20email.

The Critical Importance of Drone Detection and Mitigation for Public Safety

US Senate Judiciary Hearing

May 20, 2025

Sergeant Robert Dooley – Statewide UAS / C-UAS Coordinator

RobertDooley@FLHSMV.GOV

Florida Highway Patrol

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.

Statement for the Record

By Staff Captain Troy Wilson (Texas Rangers)

Texas Department of Public Safety

Defending Against Drones: Setting Safeguards for Counter Unmanned Aircraft Systems Authorities

Hearing Before the United States Senate Committee on the Judiciary

May 20, 2025

Introduction

Chairman Grassley, Ranking Member Durbin, thank you for inviting me to testify before you today. My name is Troy Wilson and I am Staff Captain with the Texas Rangers at the Texas Department of Public Safety. I have been conducting or overseeing criminal investigations in Texas for twenty-five years. Part of my responsibilities include overseeing drone operations for Texas Department of Public Safety (DPS).

Transnational criminal organization Unmanned Aircraft System (UAS) misuse along the Texas-Mexico border presents a significant, evolving threat. These criminal organizations are increasingly leveraging UAS technology for intelligence gathering purposes, which enables them to monitor and exploit vulnerabilities in border security operations. This includes surveillance of Texas-based border security personnel (state and federal) to coordinate illicit contraband movement and human trafficking, further intensifying the challenges faced by all law enforcement agencies.

Over the past twelve months (April 2024 to April 2025), Texas DPS-owned sensors identified 1,216 UAS border incursions. We know this is a fraction of the actual number of incidents. Alarmingly, nearly half of these UAS incursions occurred at altitudes ranging between 600 to 1,800 feet Above Ground Level (AGL)—the typical altitude range for helicopter operations.

The increasing presence of UAS operating in the same airspace as manned aviation introduces the alarming possibility of collisions, endangering citizens of the State of Texas and law enforcement personnel and equipment.

Such incidents critically impair border security efforts and endanger lives, underscoring the urgent need for enhanced detection and mitigation systems.

My written statement also includes several specific examples of drone misuse.

Existing threat

The interference with legitimate border security UAS operations by these unauthorized drones undermines critical efforts to maintain control and effectively monitor the region.

Criminal elements have also succeeded in utilizing UAS to deliver narcotics and contraband into correctional facilities including jails and prisons—posing a severe threat to the safety and

security of the inmates and staff at these locations. Beyond direct threats to people inside correctional facilities, drones are used to deliver cell phones to inmates, which are often used to coordinate criminal activity in our communities.

Furthermore, unauthorized UAS flights over critical infrastructure, such as electrical power generating plants, dams, or water treatment facilities, highlight another layer of risk, as such flights could disrupt operations or compromise public safety.

Taken together, these threats underscore the urgent need for Congress to grant authority to state and local law enforcement agencies to operate robust detection and mitigation strategies to counter the threat of drones and ensure the safety and security of the border regions.

Ongoing efforts

The Texas DPS has taken a proactive stance against the escalating threat of UAS misuse along the Texas-Mexico border. With a recent grant of $290,000 from the Office of the Governor (OOG) dedicated to detection efforts, DPS has enhanced its capabilities to address these challenges. However, as the threat continues to evolve, additional resources are crucial to ensure the effectiveness of these measures. DPS has requested an additional $210,000 to build upon this foundation and fortify its UAS detection systems.

The existing twelve (12) sensors owned by the State of Texas are limited in scope and, only detect DJI drones (DJI drones currently make up approximately 80% of the market), which means other drones go undetected and creates critical vulnerabilities that, will be increasingly exploited by the transnational criminal organizations. Moreover, the twelve sensors monitored along the border cover only approximately 180 miles, representing just 14% of the 1,254-mile stretch of the Texas-Mexico border. This illustrates the urgent need to expand sensor coverage both in terms of geography and the variety of UAS that can be detected.

Addressing these threats requires a comprehensive, layered approach. Detection technologies must be integrated to identify potential UAS threats promptly and accurately, while any mitigation strategies must be implemented with precision to minimize collateral damage. Surgical mitigation techniques are essential to neutralize threats effectively without compromising public safety or causing unintended disruptions.

Lack of personnel and resources to analyze the increasing volume of threats presents another challenge. Effective counter-UAS operations also require well-trained teams, and the current lack of training and staffing hampers timely and effective responses to incidents.

Above all, we understand that any counter-UAS detection and mitigation policy or practice must abide by any applicable state and federal laws and align with the First and Fourth Amendments.

Conclusion

Despite significant efforts at the state level, the Texas DPS faces constraints imposed by the federal government that limit the full scope of action needed to address the growing UAS threat. Nevertheless, DPS has taken a proactive approach over the past eighteen months, ensuring that all UAS personnel and recruit classes receive comprehensive training in enforcing existing drone

laws. This commitment to education and readiness reflects DPS's dedication to adapting to the evolving challenges posed by unauthorized drone activity.

Additionally, Texas DPS has actively participated in national efforts, serving on the Federal Aviation Administration's UAS Detection and Mitigation Aviation Rulemaking Committee. Through this involvement, DPS contributed valuable insights and expertise toward developing regulatory frameworks and solutions for addressing the threats posed by criminal UAS.

These actions underscore Texas DPS's commitment to innovation, collaboration, and maintaining public safety in the face of an increasingly complex, dynamic and evolving threat environment.

State and local and tribal territory law enforcement agencies need the ability to detect and mitigate criminal UAS operation along the border and near/over correctional facilities and prisons. On behalf of the Texas Department of Public Safety, we urge Congress to take action to address this issue.

I look forward to being a resource to the committee as you consider this important topic.

Thank you,

Incidents:

DPS UAS mitigated by Mexican cartel, 4/22/2025 – Laredo AOR

On April 22, 2025, at approximately 7:19 a.m., Modernization & Advanced Technology Team (MATT) notified the Laredo United States Border Patrol – Laredo Foreign Operations Branch (LRT-FOB) of an Aerial Armor alert on a drone flying across from Father McNaboe Park in Zone 5 (27.5846306, -99.5315643).

At approximately 7:25 a.m., Secretaria de la Defensa Nacional (DEFENSA) was contacted via established communications regarding the drone activity to inquire if they could respond.

At approximately 7:58 a.m., DEFENSA acknowledged the inquiry.

At approximately 8:30 a.m., U.S. Customs and Border Protection (CBP) Air Marine Operations (AMO) advised OLS UAS Team-3 (Texas Ranger Ryan Christian and DPS SOG SSgt. Luke Tkach) of a UAS operating in Mexico across from Father McNaboe Park in Laredo, TX, LRT Zone 5. AMO believed the UAS was being operated by cartel members in Mexico near GPS 27.5832969, -99.5338187.

At approximately 8:36 a.m., Team-3 located the pilot and provided photographs to AMO, who provided them to the Government of Mexico (GOM) through the CBP Foreign Operations Branch (FOB).

At approximately 8:36 a.m., Team-3 photo of the UAS pilot (black shirt) and a second male.

At approximately 8:43 a.m., photo of UAS pilot.

At approximately 8:44 a.m., a photo of a UAS pilot, the second male and a female.

At approximately 9:07 a.m., DEFENSA was contacted via established communications again due to drone activity. DEFENSA acknowledged and advised they would be responding.

At approximately 9:07 a.m., DPS UAS was notified by CBP AMO that Government of Mexico (GOM) was responding to the area.

FOB understood that DEFENSA would be deploying with UAS mitigation equipment

At approximately 9:22 a.m., DEFENSA advised that they were near the World Trade Bridge (approx. 1,536M (0.95 miles) 331° north of target) and approaching the location.

LRT Sector Intelligence Unit (SIU) received information of "chatter" near the time of DEFENSAs arrival to down any law enforcement drones. The "chatter" is believed to be from law enforcement adversaries in the area.

At approximately 9:31 a.m., DEFENSA advised the operator appeared to have landed the drone.

At approximately 9:38 a.m., Team-3 continued to monitor the pilot and a second adult male as they left their original location and traveled into the brush near the river.

At approximately 9:38 a.m., a photo of UAS pilot and a second male traveling down river away from a structure enroute to the riverbank.

At approximately 9:41 a.m., USBP Laredo North Station (LRN) Supervisor Martinez was contacted telephonically to advise of DEFENSA searching the area across from Zone 5.

At approximately 9:42 a.m., DEFENSA advised they were at the location, which is near a residence (27.5833111, -99.5337652)

At approximately 9:43 a.m., LRT-FOB coordinated a mirror patrol with Marine Unit in Zone 5 across from Father McNaboe Park.

FOB understood from established communications that DEFENSA had not had the opportunity to deploy its UAS mitigation equipment.

At approximately 9:43 a.m., while flying near GPS 27.5828898, -99.5298058 (approximately 1487 ft from the UAS pilots) at 294 ft AGL, Team-3 lost control of its UAS (TRD12H1 - DJI Mavic 3). As the UAS traveled North and dropped altitude, it would not respond to remote controller inputs. DPS SOG and TPWD SOG later recovered the UAS next to a playground in Father McNaboe Park, approximately 1,060 ft North of the location where it lost connection. The severity of damage to the UAS was catastrophic.

At approximately 11:32 a.m., DEFENSA advised that after a thorough search of the area, the search for the drone operator or drone yielded negative results. DEFENSA units cleared the area.

Suspect Drone Flight Data

Flight Id	Drone Id	Drone Type	Detection Count	Sensor Name	Max Altitude	Total Duration	Detection Time Start
113486939	F67Q3245V004L06C	Mavic 3 Pro	1	Laredo_4	1637.14	0.00	4/22/2025 4:38:50 PM
113486807	F67Q3245V004L06C	Mavic 3 Pro	27	DHS S&T 2	1640.75	20.80	4/22/2025 4:20:34 PM
113486224	F67Q3245V004L06C	Mavic 3 Pro	37	DHS S&T 2	1640.75	23.39	4/22/2025 3:38:55 PM
113485384	F67Q3245V004L06C	Mavic 3 Pro	172	DHS S&T 2	1640.75	94.03	4/22/2025 1:09:21 PM
113481441	F67Q3245V004L06C	Mavic 3 Pro	19	DHS S&T 2	1499.34	11.56	4/22/2025 9:24:30 AM
113480883	F67Q3245V004L06C	Mavic 3 Pro	67	DHS S&T 2	1467.52	19.90	4/22/2025 8:21:25 AM
113480622	F67Q3245V004L06C	Mavic 3 Pro	5	Laredo_4	1405.84	8.82	4/22/2025 7:42:22 AM
113480623	F67Q3245V004L06C	Mavic 3 Pro	88	DHS S&T 2	1416.34	20.71	4/22/2025 7:33:05 AM

Possible related UAS Incident

The day before the DPS UAS mitigation, on April 21, 2025, at approximately 8:30 a.m. Laredo Border Patrol (LRT) S-UAS had a drone malfunction near the same location (Father McNaboe Park in Zone 5 (27.5846306, -99.5315643)). The incident resulted in the LRT drone falling into the Rio Grande River.

Due to the proximity in time and location, it is suspected the LRT UAS was also illegally mitigated by Radio Frequency (RF) jamming.

LRT SIU has information indicating that since September of 2024 there have been six events related to UAS RF disruption in the Laredo Sector. Additionally, since February of 2025 there have been nine events of GPS disruption on manned aircraft in the Laredo Sector.

On April 22, 2025 in the PM hours, US Air and Marine (AMO) reported GPS disruption in its aircraft operating in LRT Zone 5 near the same area (Father McNaboe Park)

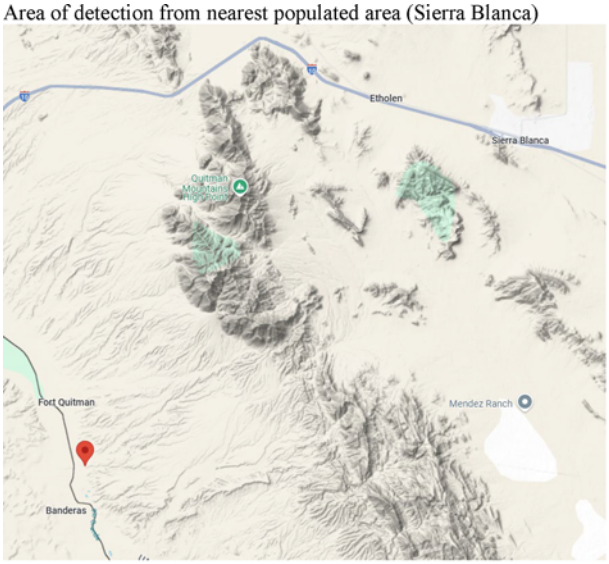
Border Patrol Drone Detection 5/6/2025

At approximately 8:55 p.m., on 05/06/2025, Sierra Blanca Border Patrol Agents in the Big Bend Sector were conducting line watch duties near an area known as "Neely's" (BBT Zone 1) and witnessed two drones hovering above them. The agents stated they observed the drones spray a mist or fog which gave the drones a strange fuzzy appearance (See photo below). The two drones hovered above the agents for a few minutes, turned off their lights and flew north away from the agents and the US/ Mexico Boundary line. BBT air domain awareness (Dedrone) did not pick the drones up at the time of the detection by the agents. AMOC was called and they stated that they were also unable to detect anything in the area as well. An MC-L was sent north of the area in an attempt to spot the drones but were unable to detect them. The agents stated that the drones were high enough they did not feel threatened by whatever was being sprayed. The videos are hard to see but clearly show the fuzzy appearance of the drones, but the attached picture shows a clear view of the drone (see below).

The area where the detection occurred is a desolate area with little to no roadways and very few residents (in the US and in Mexico). The area is also a few miles east of an area where several vehicle incursions have occurred in the Fort Hancock Border Patrol Station AOR (El Paso Sector). This is the second night in a row that drones were detected near the river, a drone incursion occurred the previous night several miles east of this area which was witnessed by DOD personnel utilizing the camera system on their Stryker vehicle.

Detection occurred approximately 1697.80 feet from the US/Mexico boundary.

Area of detection from nearest populated area (Sierra Blanca)

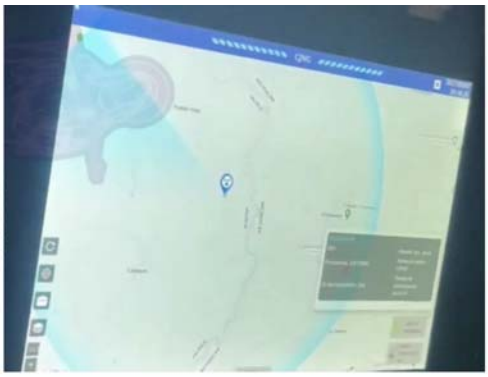


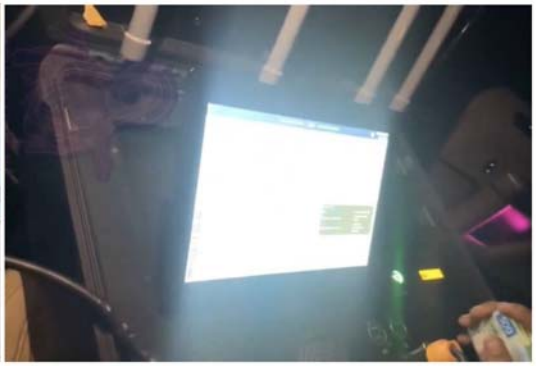
Close-up of drone as it is spraying.

Arizona HIDTA "KNNR" report, dated May 5, 2025 (Mexico)

- First DOCUMENTED potential use of a FPV (First Person View) use in Mexico. The drone is a DJI Avata 2, which is a FPV drone. If this is truly video from Mexico, this would be the first time of a FPV drone being used by cartels in conflict. (pg 14)

- CJNG sicarios operating a Chinese manufactured VBE 1PD drone detector. This system can be used to detect & direction find drones & operators. Special Forces member of CJNG filming himself while operating a signal jammer that can have different uses, including interrupting the signals of radios, cell phones, and sometimes even drones. (pg 14)



- Video showing a Carteles Unidos drone with an explosive device being used to battle CJNG in Michoacán. (pg 66)

- Two types of drone munitions seized by authorities. These munitions are crude in design. They appear to have PVC bodies w/ an end cap that has four stabilizer fins of corrugated plastic glued together on the bottom, ~26 cm in length. (pg 67)

- Filmed by La Familia Michoacana (LFM) sicarios. The drone is a DJI Matrice 350 RTK & Zenmuse H20 or H30 camera w/ munition attached to the body. Munition is large, made of unknown materials w/ a body & attached stabilizer fin section. DJI Matrice 350 RTK has a height of 43 centimeters. This would mean that the drone drop munition is at least 43 centimeters in length. This is on the larger side of drone drop munitions that are typically seen in cartel videos on social media. (pg 70)

August 22, 2022 (www.dronedj.com)

Texas prison drone drug-smuggling ring busted, netting 42 suspects

Texas prison drone drug-smuggling ring busted, netting 42 suspects

Once tipped to the activity, the TDCJ joined with an array of law enforcement agencies to investigate the ring's use of drones to deliver drugs and other contraband into prisons.

This news out of Texas came in the wake of arrests in Georgia of two men now facing charges of having smuggled drugs, including 280 grams of meth, into state prisons by drone. Use of drones

to smuggle drugs and other contraband into prisons has become a major plague for authorities around the US and abroad.

The same problem is on the rise in Texas, where the Department of Justice's Office of Inspector General released an audit indicating a 50% surge in drone activity near or above Bureau of Prisons (BOP) in 2020 alone. The findings noted it number of sightings it worked from is almost certainly lower than the actual number of flights that take place around the banned airspaces of penitentiaries.

"We found that the BOP faces significant and growing challenges to protect its facilities from drone threats," the audit read. "Drones have been used to deliver contraband to inmates, but could also be used to surveil institutions, facilitate escape attempts, or transport explosives."

October 6, 2022 (cbsnews)

Texas man pleads guilty to flying drone into Fort Worth prison yard - CBS Texas

Man flew drone loaded with drugs, electronics and other contraband into a Fort Worth prison yard has pleaded guilty.

Included in the contraband was methamphetamine, THC, tobacco, cell phones and mp3 players. According to court documents, the drone crashed inside a secure, fenced-in yard near the prison's HVAC shop, where it was recovered by staff.

When he was arrested in August, Henderson was charged with one count of attempting to provide contraband in prison, one count of serving as an airman without an airman's certificate, and one count of possession with intent to distribute a controlled substance.

Plea papers show Henderson admitted to flying a drone loaded with contraband into the airspace of Federal Medical Center Fort Worth. Court documents say that affixed to the drone was a package containing 46 grams of crystal methamphetamine, 87 grams of pressed THC, two prepaid smartphones, and nine mp3 players.

"The criminal element will always take advantage of new opportunities for illegal activity as technology progresses," said FBI Dallas Special Agent in Charge Matthew J. DeSarno. "In this instance, excellent collaborative investigation among federal and local agencies led to federal charges and prevented contraband from entering the federal prison system."

There is also surveillance video from a nearby high school that showed Henderson driving up in a red Chevy Tahoe, removing a drone and a package from the vehicle, launching it towards the prison and driving off.

Prison staff reportedly found the drone controller, immediately paring it with the device.

The drone showed flight logs, of which investigators identified four flights entering FMC Fort Worth's airspace. Investigators also saw two flights that entered the airspace over Federal Correctional Institution Seagoville and another correctional center southeast of Dallas.

Cell phone records of Henderson's also show that the phone was near FMC Fort Worth around the time of the drone crash and near FCI Seagoville near the time of the drone's flight into the prison's airspace.

According to the FAA's database, Henderson did not have an airman's certification and the drone he used was registered to another owner who cancelled their registration in August 2018.

September 26, 2023 (abc13 news)

https://abc13.com/drone-drug-drops-grant-parish-louisiana-fugitives-surrender-harris-county-federal-prison-smuggling/13832220/

HARRIS COUNTY, Texas (KTRK) -- A man and a woman, who are accused in a scheme to get drugs into federal prisons across the U.S., turned themselves in to the Harris County Jail on Tuesday afternoon.

The sheriff's office in Grant Parish said it uncovered the scheme during a traffic stop near the federal prison in Pollock, Louisiana, almost three weeks ago.

According to Sheriff Steven McCain, deputies found $1.18 million worth of K2-soaked paper, $10,000 worth of Suboxone, $4,000 worth of THC wax, and $1,500 worth of marijuana. They also found two drones and numerous drone batteries, eight cell phones, a vacuum sealer, and a scale.

"You can see these orange drones in front of me," Sheriff McCain said during a news conference. "Law enforcement recovered these drones, it was being used to drop the stuff across the fence inside of the fence of the federal prison. The cans weren't open like this when they were discovered. These were filled with drugs. These drone has an actuator on there that the operator pushes a button on the remote control and releases the package."

McCain also shared a text message with a list of what was supposed to be dropped at a certain prison facility.

"They had a very, very specific list of what was supposed to be dropped at every location," the sheriff said.

October 7, 2024 (abc 12 news)

Drone used to bring contraband into federal prison confiscated | 12newsnow.com

Jefferson County deputies confiscate drone used to bring contraband into United States Penitentiary

Some of the contraband that deputies confiscated along with the drone includes cell phones, drug paraphernalia, watches, Narcan, spray paint and various electronics.

BEAUMONT, Texas — Jefferson County deputies have confiscated a drone that the sheriff's office says was used to bring contraband into the United States Penitentiary, in Beaumont.

Some of the contraband that deputies confiscated along with the drone includes cell phones, drug paraphernalia, tobacco, GPS trackers, credit cards, a shank, watches, Narcan, spray paint and various electronics.

Two people were arrested in a car outside the jail and the car was towed. Jefferson County Sheriff Zena Stephens says incidents like these happen more often than you think.

"We have ranchers who call us many times in the county, because they see the drones flying over, and they see the drop offs," said Stephens.

Patrol Deputy Adam Lovett with Jefferson County Sheriff's Office told 12News that he pulled a man and woman over for speeding on Hillebrant Road and began questioning why they were speeding. Both gave conflicting responses, prompting a search of vehicle, which the driver refused.

"He said they were down here for work, then I went and spoke with the female in the passenger seat. She told me they were down here visiting some friends, so right there you have conflicting stories," said Lovett.

They called out a K9 unit, who was alerted to something during the search. That’s when they found contraband and arrested the couple for drug possession.

Some of the items were wrapped in a way that hid what the item was along with fishing line believed to be used for the drop of contraband into the federal prison. The vehicle was located near the back of the prison.

"I was shocked there was that much. I figured I was just going to find a little bit of meth or something, never thought I'd come across a little enterprise they have going on," Lovett told 12News.

Stephens believes they planned to fly the contraband into the prison for inmates. She says it's a problem they've seen before.

"They'll bundle it in plastic, paper, backpacks, cases and when the drone drops the packaging in the prison area it doesn't get any attention. This not our first and it is certainly not our last," said Stephens.

As smugglers continue to revolutionize their tactics Sheriff Stephens wants people to report any drones they see flying close to the prison.

SENATOR MIKE LEE QUESTIONS FOR THE RECORD
Prof. Laura K. Donohue

(1) What constitutional concerns, if any, do you see with the current federal counter-UAS regime as applied to sensitive locations such as federal prisons, the border, federal buildings, and airports?

Response:
Current counter-UAS authorities, codified at 6 U.S.C. § 124n, raise troubling First, Fourth, and Tenth Amendment concerns.

The statute's broad definition of a "covered facility or asset" and its authorization to "detect, identify, monitor, and track" UAS and to control, seize, confiscate, disable, damage, or destroy drones risk putting the Secretary of Homeland Security and the Attorney General in the position of preventing citizens and media from engaging in audio and video observation and recording of government actions in public space, which courts recognize as protected First Amendment expressive activity.[1] The statutory definition of covered facilities includes all Department of Homeland Security missions related to Customs and Border Protection (including along the border, which under federal regulations constructively extends 100 miles inside the United States) as well as efforts to protect any "buildings, grounds, and property that are owned, occupied, or secured by the Federal Government."[2] This would include any federal activity along the borders as well as within hundreds of miles from any international airport, or near any federal facility, across the United States. The statute also includes all Department of Justice missions pertaining to buildings or grounds leased or owned by the department, as well as Federal courts, again potentially sweeping in a significant amount of activity which citizens otherwise have the right to observe.[3] The decision of which facilities to subject to enhanced protections, and the duration, is left entirely up to the executive. Because the Attorney General's guidelines implementing 6 U.S.C. § 124n requires the government to assess the content and nature of events which require threat-mitigation efforts, the provisions trigger strict scrutiny.[4] Even under intermediate scrutiny, current counter-UAS provisions burden substantially more speech than necessary by allowing the government to disrupt, seize, or destroy drones without regard to distance, activity, or property rights.[5] Taken together, current drone provisions risk having a chilling effect and restricting the ability that undergirds one of the primary aims of the First Amendment, which is to hold officials accountable.[6]

Current counter-UAS laws also raise Fourth Amendment concerns because they empower the government to intercept drones and search their contents without a warrant. The statute gives the federal government the authority to access all communications between the drone operator and

---

[1] *See, e.g.,* ACLU of Ill. v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2014) ("The act of making an audio or audiovisual recording is necessarily included within the First Amendment's guarantee of speech and press rights as a corollary of the right to disseminate the resulting recording."); People for the Ethical Treatment of Animals, Inc. v. N.C. Farm Bureau Fed'n, Inc., 60 F.4th 815, 82434 (4th Cir. 2023).
[2] 6 U.SC. § 124n(k)(3)(C)(i), referencing 40 U.S.C. § 1315(a).
[3] *See* 6 U.SC. § 124n(k)(3)(C)(ii).
[4] William Barr, Attorney Gen., Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems, at III(a) (April 13, 2020), X(F), https://www.justice.gov/archives/ag/page/file/1268401/dl?inline (defining a National Special Security Event as "a designated event that, by virtue of its political, economic, social, or religious significance, may be the target of terrorism or other criminal activity.")
[5] *See* 6 U.S.C. § 124n (b)(1)(C)–(F).
[6] *See* Turner v. Lieutenant Driver, 848 F.3d 678, 689 (5th Cir. 2017).

the UAS, as well as to disrupt and control all UAS systems.[7] The government can seize not just communications directing the drone where to fly, but also communications related to what the drone itself is collecting, observing, and communicating back to the drone operator. It also means that the government may gain access to any devices used over the course of such transmissions, whether it be radio frequency signals, Wi-Fi, or satellites, which play a critical role in communicating with drones.[8] Lacking any statutory limits, the current counter-UAS regime essentially operates as a general warrant. To address these issues, counter-UAS laws moving forward should operate within the limits of current Constitutional restraints and set clear boundaries of what information the government may access without warrants.

Lastly, the statute risks intruding on traditional state police powers over low-altitude airspace and property rights. Federal authority over navigable airspace is clear, but states retain sovereignty over drones operating at low altitudes above state and private land.[9] Current counter-UAS laws risk encroaching on such state authority.

(2) You have analogized the collection of information from drones to practices under the Foreign Intelligence Surveillance Act (FISA). Could you expand on how you see these two being related, and what lessons from FISA reform Congress could apply to forthcoming counter-UAS legislation?

Response:
Both FISA and § 124n aim to address national security threats. Unlike FISA, however, the counter-UAS regime lacks prior judicial review. In *U.S. v. U.S. District Court*, the Supreme Court held that electronic surveillance inside the United States on matters related to domestic security must satisfy some sort of warrant procedure in which a neutral and detached magistrate plays a role.[10] As the court explained, "The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute."[11]

Congress responded with the Foreign Intelligence Surveillance Act of 1978, under which the government must demonstrate probable cause that the target is a foreign power or an agent thereof, and probable cause that the target is likely to use the facilities to be placed under surveillance, prior to interception.[12] The determination is made by an Article III judge appointed by the Chief Justice to the Foreign Intelligence Surveillance Court.[13] Surveillance is only approved for limited periods.[14] The statute gives the government the flexibility to respond in an emergency, followed by application within seven days to the court for an order to continue surveillance.[15] Any U.S. person information obtained must comport with the standard minimization procedures and, if requested by the court, additional protective measures to ensure that information is neither retained nor disseminated in a matter that undermines the Fourth

[7] *See* 6 U.S.C. § 124n(b)(1)(A), (C),(D).
[8] *See* 18 U.S.C. § 2510 (1).
[9] *See* United States v. Causby, 328 U.S. 256, 265 (1946); Griggs v. Alleghany, 369 U.S. 84, 85 (1962).
[10] United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 323–24 (1972) (Keith).
[11] 407 U.S. at 317.
[12] *See* 50 U.S.C. § 1805(a). Every court to consider the Constitutionality of FISA has found it sufficient. *See, e.g.,* United States v. Nicholson, 955 F. Supp. 588, 590-91 (E.D. Va. 1997); United States v. Cavanagh, 807 F.2d 787, 790–92 (9th Cir. 1987); United States v. Duggan, 743 F.2d 59 (2d Cir.1984); United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982). *See also* Ellsberg v. Mitchell, 709 F.2d 51, 66 n. 66 (D.C. Cir. 1983) (noting that FISA had theretofore survived all constitutional challenges), cert. denied, sub nom. Russo v. Mitchell, 465 U.S. 1038 (1984).
[13] *See* 50 U.S.C. §§ 1803(a)(1); 1805(a)(2).
[14] *See* 50 U.S.C. § 1805 (d)(1).
[15] *See* 50 U.S.C. § 1805(e)(1).

Amendment.[16] If surveillance is directed at a different facility over the course of the surveillance, the government must promptly inform the court, transmitting additional information.[17] Any judicial opinions which result in a significant interpretation of the law must then be reported to Congressional committees, and annual statistics must be provided to Congress on various aspects of government use of the authorities, such as the number of applications, any full or partial denials, and the number of applications granted.[18] Finally, the court has the possibility of appointing amici curiae for any novel matters of law.[19]

In contrast, as it currently stands, 6 U.S.C. § 124n operations require only the approval of the Deputy Attorney General or, in emergencies, the head of an authorized agency.[20]

Implementing FISA-like procedures that protect constitutional rights, where, outside of exigent circumstances, agencies would need to demonstrate some sort of probable cause to a third party magistrate before taking action against a drone, any U.S. person information collected would be minimized, significant interpretations of law would be presented to Congress, and statistical information would be made available could and should apply to any future counter-UAS legislation.

(3) In your testimony, you raised Tenth Amendment concerns about the federal counter-UAS regime potentially abridging state sovereignty. What do you see as the proper balance between federal and state authority in the counter-UAS domain?

Response:
Distinguishing between higher navigable airspace, where federal authority for air commerce is clear, and the low-altitude space where state police powers and property rights have been traditionally recognized would give the federal government the authority to protect federally-owned property and higher, navigable airspace without raising Tenth Amendment concerns. Almost every state has already implemented drone laws, many of which already address the concerns raised at the federal level.[21] States should continue to exercise their traditional power to manage UAS activity in low-altitude airspace over state and private land and forthcoming legislation should complement, not overrule, these efforts.

---

[16] *See* 50 U.S.C. § 1805(a)(3).
[17] *See* 50 U.S.C. § 1805(C)(3).
[18] *See* 50 U.S.C. §§ 1871(a)(1), 2, 4, 5.
[19] *See* 50 U.S.C. § 1803(i).
[20] William Barr, Attorney Gen., Guidance Regarding Department Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Systems, at III(a) (April 13, 2020), X(D), https://www.justice.gov/archives/ag/page/file/1268401/dl?inline.
[21] *See* Federal Aviation Administration, Updated Fact Sheet (2023) on State and Local Regulation of Unmanned Aircraft Systems (UAS) https://www.faa.gov/sites/faa.gov/files/State-Local-Regulation-of-Unmanned-Aircraft-Systems-Fact-Sheet.pdf (noting "at least 44 States have enacted laws relating to UAS, addressing issues such as privacy, delivery of prison contraband, firefighting, law enforcement use of UAS, and UAS registration.").

A P P E N D I X

The following submissions are available at:

https://www.govinfo.gov/content/pkg/CHRG-119shrg61982/pdf/CHRG-119shrg61982-add1.pdf

Submitted by Chair Grassley:

Submitted by Ranking Member Durbin:

Submitted by Senator Schmitt: