Department of Justice

STATEMENT OF

BRAD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

AND

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

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED

"Safeguarding the Homeland from Unmanned Aerial Systems"

PRESENTED

DECEMBER

10, 2024

STATEMENT OF
BRAD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

AND
ROBERT W. "WES" WHEELER, JR.
ASSISTANT DIRECTOR, CRITICAL INCIDENT RESPONSE GROUP (CIRG), FEDERAL BUREAU OF INVESTIGATION

BEFORE THE
COMMITTEE ON HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

AT A HEARING ENTITLED
"SAFEGUARDING THE HOMELAND FROM UNMANNED AERIAL SYSTEMS"

PRESENTED
DECEMBER 10, 2024

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

I. The Threat Posed by Misuse of Drones

A. The Threat Continues to Grow

The use of UAS technology in the United States continues to grow rapidly. Along with significant benefits come significant risks. Commercial use of UAS already generates billions of dollars in economic growth. As of October 1, 2024, over 791,000 UAS in the United States are

registered with the Federal Aviation Administration ("FAA") with more drones required to be registered that simply are not. Law enforcement and public safety use of UAS allows officials to perform critical missions, from accident rescues to tactical incursions, while reducing risk to personnel and the public.

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

- platforms designed or modified to conduct kinetic attacks using payloads of explosives, firearms, or weaponized chemical, biological, or nuclear material;
- cyber-attacks against wireless devices or networks;
- espionage;
- the illicit trafficking of narcotics and contraband; and
- monitoring law enforcement activity.

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

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

- (i) In November 2024, the Department arrested and charged Skyler Philippi of Columbia, Tennessee, with attempting to use a UAS as a weapon of mass destruction to destroy an energy facility. Philippi had conducted research on past attacks on the U.S. electrical system and allegedly concluded that attacking with firearms would not be sufficient; instead, he planned to use a UAS laden with explosives. He allegedly planned to use the UAS to attack the power grid, leaving thousands of Americans and critical infrastructure like hospitals without power. As alleged, Philippi was a self-styled "accelerationist" who hoped his actions would "shock the system" and lead to civil unrest.[i]

    - Importantly, current law does not contain clear authority for the federal government, SLTT law enforcement, or the private sector to mitigate or, for certain technologies, even detect UAS that threaten critical infrastructure.

- (ii) Also in November 2024, Edward Kelley of Maryville, Tennessee, was convicted of a conspiracy to murder federal employees, in part through the planned use of weaponized drones. While awaiting trial for crimes he committed at the United States Capitol on January 6, 2021, Kelley planned an attack on the

Knoxville FBI Field Office that would have used car bombs and incendiary devices appended to drones as revenge against law enforcement for his prior arrest.[ii]

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

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

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

B. The Threat Posed to Prisons

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

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

C. FBI Protection of Mass Gathering from the UAS Threat

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

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

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

II. The Administration's Consolidated C-UAS Legislative Proposal

A. Overview of the Administration Proposal

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

Specifically, the Administration's proposal would expand the current § 124n authority in targeted ways based on our experience under the law and our assessment of the growing threat. Current § 124n authority will lapse this month, so our existing programs must be reauthorized to avoid shutting down FBI's ability to protect mass gatherings. The authority is essential because, without it, use of the most effective types of UAS detection and C-UAS technologies could violate

criminal laws, including those that prohibit destroying or disabling aircraft and intercepting signals and communications. *See, e.g.*, 18 U.S.C. § 32 (the Aircraft Sabotage Act); 18 U.S.C. §§ 2510 *et seq*. (the Wiretap Act, also known as Title III); 18 U.S.C. §§ 3121-3127 (the Pen/Trap Statute).

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

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

B. Authorizing Limited SLTT C-UAS Programs

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

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

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

only" authority would provide significant public safety benefits and could be safely employed today.

(ii) Mitigation Pilot

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

C. Expanding Coverage to Airports and Critical Infrastructure

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

D. Mutual Support Authority

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

E. Prisoner Transports

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

F. Expanding Protections for Privacy and Civil Liberties

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

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

G. Sunset

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

Conclusion

In closing, the proposed legislation by itself will not eliminate the threats presented by malicious or irresponsible use of drones. However, it will significantly enhance our ability to mitigate this threat in a manner that is measured, responsible, and consistent with the FAA mandate to integrate drones safely into the national airspace system. As the United States seeks to lead the world by integrating uncrewed aviation into the national airspace, Congress must

build security into the frameworks that support UAS integration by ensuring that those responsible for protecting the public have the authority they need to do so. Integration and security must go together.

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

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

***

[i] https://www.justice.gov/opa/pr/man-arrested-and-charged-attempting-use-weapon-mass-destruction-and-destroy-energy-facility
[ii] https://www.justice.gov/opa/pr/federal-jury-convicts-man-conspiring-murder-fbi-employees#
[iii] https://www.startribune.com/u-student-from-china-receives-6-month-prison-term-for-taking-drone-photos-over-naval-shipyard/601162150
[iv] https://www.justice.gov/usao-cdca/pr/lancaster-man-arrested-charges-he-used-drone-fly-fentanyl-including-customer-who-later
[v] https://nij.ojp.gov/topics/articles/addressing-contraband-prisons-and-jails-threat-drone-deliveries-grows
[vi] https://www.justice.gov/usao-sdms/pr/tennessee-man-pleads-guilty-using-drone-fly-marijuana-yazoo-city-federal-correctional
[vii] https://www.justice.gov/usao-sdga/pr/pair-indictments-charge-conspiracies-use-drones-deliver-illegal-drugs-contraband-cell
[viii] https://www.justice.gov/usao-edca/pr/four-indicted-scheme-deliver-drugs-state-prisons-drone
[ix] https://www.justice.gov/usao-md/pr/pennsylvania-man-facing-federal-felony-charges-illegally-operating-drone-during-national
[x] https://www.justice.gov/usao-ma/pr/boston-man-charged-violating-national-defense-airspace

The 'Drone Wars' in Ukraine—And What it Means for America

Written Testimony of Dr. Paul Schwennesen

Before the U.S. House of Representatives Subcommittee on Counterterrorism, Law Enforcement, and Intelligence and Subcommittee on Transportation and Maritime Security

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

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

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

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

The United States is rapidly and unwittingly losing its strategic military advantage in this new technical environment. There can be little doubt that China, North Korea, Iran, and other emergent powers are eagerly sending observers and technicians to the frontlines in occupied Ukraine to carefully note the revolution in weapons delivery and to adopt it into doctrines which

seek to invert the military strengths of their larger, better equipped, better trained western geopolitical adversaries.

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

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

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

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

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

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

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

Scenarios:

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

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

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

Testimony of

Keith Jones
Deputy Executive Assistant Commissioner
Air and Marine Operations
U.S. Customs and Border Protection
Department of Homeland Security

For a Hearing on

"Safeguarding the Homeland from Unmanned Aerial Systems"

Before the

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Counterterrorism, Law Enforcement, and Intelligence
and
Subcommittee on Transportation and Maritime Security

December 10, 2024
Washington, D.C.

Introduction

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

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

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

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

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

---

[1] The term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system. *See* 49 U.S.C. § 44801(12).

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

Threats to U.S. Border Security from the Malicious Use of UAS

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

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

TCOs and other malicious actors use UAS to conduct reconnaissance of CBP personnel and operations to pass information to contacts on the ground to assist such contacts in determining where to guide noncitizens or transport contraband. The use of drones for illicit cross border activity is not only widespread, but highly organized and integrated into TCO operations. This illicit activity threatens the safety of our frontline personnel, poses a collision risk to our aircraft, and adversely affects our border security operations.

Current CBP C-UAS Authority and Operations

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

Among other things, and notwithstanding select criminal provisions from which section 124n offers relief, the Act authorizes the Secretary of Homeland Security to provide DHS personnel with certain assigned duties (i.e., certain CBP personnel), specific statutory relief necessary to perform the C-UAS protective mission. The statute allows CBP to take certain actions to detect, identify, monitor, track, and mitigate UAS which pose a credible threat. The actions authorized in the Act include electronic detection, electronic mitigation through communications signal intercept and interruption, kinetic/physical mitigation, and device seizure. This authority expressly enables the protection of "covered facilities or assets" identified by the Secretary in coordination with the Secretary of Transportation[6] from credible UAS threats that relate to specific DHS mission sets, including CBP security and protection missions. The Act also authorizes protection of shared DHS

[3] Between October 1, 2024, and November 16, 2024.
[4] Any drone detected within 500 meters of either side of the border.
[5] The term "counter-UAS system" means a system or device capable of lawfully and safely disabling, disrupting, or seizing control of an unmanned aircraft or unmanned aircraft system. *See* 49 U.S.C. § 44801(5). Although this term, as defined in statute, does not encompass UAS detection, references to "C-UAS" activities throughout this testimony are intended to include both UAS detection and mitigation activities including those that do not require relief from federal criminal laws.
[6] Defined in the Preventing Emerging Threats Act as any facility or asset that is identified as high-risk and a potential target for unlawful unmanned aircraft activity by the Secretary or the Attorney General, in coordination with the Secretary of Transportation with respect to potentially impacted airspace, through a risk-based assessment; is located within the United States; and directly relates to a select authorized DHS mission, or authorized joint DHS or DOJ mission, *See* 6 U.S.C. § 124n(k)(3).

and Department of Justice (DOJ) mission sets including protection of National Special Security Events (NSSE) and Special Event Assessment Rating (SEAR) events; provision for support to state, local, territorial, tribal, or campus law enforcement (upon request of the chief executive officer of the respective state, tribe, or territory) for mass gatherings that are limited to a specific timeframe and location; and protection of an active federal law enforcement investigation, emergency response, or a security function that is limited to a specified timeframe and location.

Consistent with the Act and the DHS Secretary's policy guidance, CBP implemented a C-UAS policy and, subsequently, its first operations plan to designate the Yuma Border Patrol Sector as a "covered facility or asset" in July 2020 after extensive discussion and review to ensure lawful and efficient operational implementation. CBP is committed to conducting its C-UAS activities with precision, identifying and targeting illicit activity while safeguarding lawful commercial and recreational drone use.

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

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

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

[7] Generally, mitigation involves disrupting the signal between a drone and its controller, causing the drone to activate its pre-programmed recovery protocol, such as returning to its designated "home" location or hovering in place. If this action does not neutralize the threat, certain C-UAS systems can emulate the controller to redirect the drone to a secure or DHS-preferred location.
[8] As of November 16, 2024.

C-UAS Policy and Authorization Process

To standardize the application of C-UAS authorities, DHS established a C-UAS Program Management Office (PMO) within the Office of Strategy, Policy, and Plans (PLCY). The PMO coordinates CBP's C-UAS activities to ensure alignment with Departmental policy and serves as the primary liaison for interagency partners, particularly DOT and the FAA.[9]

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

Privacy, Civil Rights, and Civil Liberties Protections

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

Pursuant to the Act, CBP may intercept or acquire command and control communications from a UAS, but only to the extent necessary to support C-UAS actions authorized by the DHS Secretary to protect a designated covered facility or asset. CBP may only intercept, acquire, access, maintain, or use communications to or from a UAS in a manner consistent with the First and Fourth Amendments to the Constitution and applicable federal laws and Department policies. In addition to those privacy protections in the Act, DHS applies Section 222 of the Homeland Security Act of 2002, as amended, to require all Component C-UAS programs to submit a Privacy Threshold Assessment (PTA) and obtain DHS Privacy Office approval prior to deploying C-UAS technology. The Privacy Office uses the PTA to determine the need for a Privacy Impact Assessment (PIA), which includes measures to mitigate privacy risks. DHS has published multiple C-UAS PIAs for public consumption consistent with requirements outlined in the Homeland Security Act of 2002.[10]

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

---

[9] The FAA is statutorily responsible for the safe and efficient management of the navigable airspace of the United States.
[10] *See, e.g.,* https://www.dhs.gov/publication/dhsallpia-085-counter-unmanned-aircraft-systems-c-uas.

The Future Landscape of UAS Threats

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

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

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

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

Statement of

Cathy L. Lanier
Chief of Security
National Football League

before the

Subcommittee on Counterterrorism, Law Enforcement, and Intelligence
Subcommittee on Transportation and Maritime Security Subcommittee
Committee on Homeland Security
United States House of Representatives

December 10, 2024

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

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

I last had the privilege of testifying in September 2018, before the Senate Committee on Homeland Security and Government Affairs when Congress was considering this same issue. Congress subsequently included the Preventing Emerging Threats Act in the FAA Reauthorization Act of 2018. That law took an important first step in protecting the homeland against rogue drones by providing counterdrone authority to federal law enforcement officials at

the Department of Justice and the Department of Homeland Security. Back then, and ever since, the NFL and other sports leagues have urged Congress to enact legislation that would take the appropriate next steps to meet this growing threat by providing counterdrone authority to state and local law enforcement officials, which are the entities that actually lead the work to provide safety and security at nearly all of our stadiums. They are at the frontline providing on-the-ground protection to fans, players, and stadium and event officials. To be clear: We are not seeking mitigation authority for the NFL or other sports organizations. We seek that authority for the law enforcement partners with whom we work in ensuring a safe and secure environment for our events.

Drone Incursions Are Growing

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

These incursions at NFL games included the following:

- In 2019, during the Super Bowl in Atlanta, an FBI team detected a drone in the restricted airspace moments before six Air Force F-16s prepared to conduct a flyover before the game. Fortunately, the FBI team was able to communicate with the flyover team to prevent a collision.

- A Ravens vs. Bengals game was delayed in November 2023 because of a drone flying over the stadium bowl. After stadium authorities detected the drone, state law enforcement officials were notified and located the drone operator, who was interviewed by officials, including local FBI agents.

- In January 2024, the AFC championship game between the Ravens and the Chiefs was paused because a drone violated the restricted airspace. Stadium authorities notified state law enforcement officials, who located the drone operator. The drone operator was questioned by state and federal law enforcement and charged with three felony counts related to operating an unregistered drone, serving as an airman without a certificate, and violating national defense airspace. The operator subsequently pled guilty to a misdemeanor.

Each and every one of these incursions violated longstanding law. Following the terrorist attacks of September 11, 2001, the FAA established flight restrictions over stadiums and other large gatherings. Congress subsequently strengthened and codified these requirements. The current version of the temporary flight restriction prohibits all aircraft operations over certain

sporting events from one hour before until one hour after the event, from ground level to 3,000 feet, and within a radius of three nautical miles. In addition to NFL games, this flight restriction applies to Major League Baseball games, NCAA Division I football games, and NASCAR, Indy Car, and Champ Series races. The flight restrictions designate the airspace as National Defense Airspace, and any operator who knowingly or willfully violates the flight restriction may be subject to criminal penalties.

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

Our national security and intelligence agencies continue to warn that terrorist groups and other bad non-state actors consider stadiums and other mass gatherings attractive targets for attack. In fact, earlier this year, Islamic State propaganda specifically encouraged attacks on stadiums, including referencing the Paris Summer Olympics. And social media posts recently threatened drone attacks at the Cricket World Cup on Long Island, New York.

H.R. 8610, the Counter-UAS Authority Security, Safety, and Reauthorization Act

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

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

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

We appreciate that the bill provides for a pilot program for state and local law enforcement counterdrone capabilities, and that the proposal explicitly includes stadiums in the definition of covered sites. As amended, the bill limits the pilot program to only five agencies, potentially expanding to fifteen, and further limits the program to just four covered sites per agency. First, we strongly recommend expanding the pilot program to adequately protect fans

attending major sporting events. Specifically, we encourage the Committee to increase the number of agencies and remove the cap on the number of sites that each agency could protect. These changes would better help us protect more fans in more places in a more expeditious timeframe across the country.

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

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

Congress Should Prioritize Enacting Counterdrone Authority for the Stadium TFR

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

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

Furthermore, Congress, the FAA, and national security agencies have made considerable strides in implementing a comprehensive regulatory structure for drone operations that lay the groundwork for immediately expanding counterdrone authority to state and local law enforcement to protect stadiums during live events. These steps included implementing Remote ID, adopting a comprehensive program for remote pilot certification, creating registration and

labeling requirements for drones, and implementing Congress's modification of the hobbyist exemption, all of which the sports leagues supported.

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

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