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