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.