Testimony of
Samantha Vinograd
Assistant Secretary (Acting) for
Counterterrorism, Threat Prevention, & Law Enforcement
Office of Strategy, Policy, and Plans
Department of Homeland Security

on

Protecting the Homeland from Unmanned Aircraft Systems

Before

The United States Senate
Committee on Homeland Security and Governmental Affairs

Washington, D.C.
Thursday, July 14, 2022

Chairman Peters, Ranking Member Portman, and distinguished Members of the Committee, thank you for inviting me to testify regarding the current authority for the Department of Homeland Security (DHS) and Department of Justice (DOJ) to counter threats from unmanned aircraft systems (UAS[1] or "drones") and proposed legislation to reauthorize and expand the authority. This legislation is essential for DHS and DOJ to continue critical missions to protect national security and public safety, while remedying major gaps in our counter UAS (C-UAS) authority, so we can keep pace with the dynamic and evolving threat environment.

Today, I am here with my partners from DOJ and the Federal Aviation Administration (FAA) to ask for your help. During the past four years, DHS and DOJ have judiciously implemented the C-UAS authority that Congress granted through enactment of the *Preventing Emerging Threats Act of 2018* (the Act) while ensuring the protection of privacy, civil rights, and civil liberties. Through numerous deployments, DHS and DOJ also have demonstrated the safe exercise of C-UAS authority, with extensive coordination with the FAA, and minimized impacts to the national airspace system. Congressional action is urgently required, as DHS and DOJ authority to detect and counter drone threats will expire in less than three months on October 5, 2022. A lapse in our authority would result in perilous and unacceptably high national security and public safety risks. Sustaining and enhancing C-UAS authority is the foundation of the security architecture necessary to continue the integration of drones into the national airspace and for commercial purposes, which will yield substantial benefits to our economy and way of life.

Technological advances have accelerated drone capabilities across military, commercial, and recreational applications. Their compact size and often low cost make them suitable for many beneficial and critical uses, including minimizing safety risks for critical tasks previously done by humans. Drones are playing a transformative role in transport and delivery, critical infrastructure management, agriculture, search and rescue, disaster response, public safety, coastal security, military operations, journalism, entertainment, and others. Estimates suggest that rapidly advancing drone technology and integration will result in new innovations and generate significant economic growth and opportunity for businesses and private citizens. To be clear, DHS supports the lawful use of drones, including by commercial and recreational users, which constitute the vast majority of UAS users. Like all technology, however, drones can be exploited for malicious use, threatening national security and public safety, which is DHS's concern.

My testimony will address four points: (1) describe the evolving threat environment and domestic drone incident data; (2) summarize DHS's current C-UAS authority and major gaps; (3) explain the Administration's legislative proposal to reauthorize and expand C-UAS authority and why it is necessary; and (4) highlight how DHS will continue to responsibly implement, use, and ensure oversight of C-UAS authority.

[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)

Dynamic and Evolving Threat Environment Is Increasing and Diversifying

As drone usage proliferates and integration into the national airspace system progresses, threat actors are increasing and diversifying their malicious use, and errant actors are increasingly interfering with manned aviation. The threat can take several forms, which I will describe and place in context with domestic drone incident data.

- Globally, drones continue to be used by adversaries **as a weapon**. This threat vector is a major concern for protecting mass gatherings and VIPs and is a major reason Congress provided C-UAS authority to DHS and DOJ nearly four years ago. Abroad, threat actors have used drones to attempt assassinations of the Venezuelan president in 2018 and Iraqi prime minister in 2021. In Mexico, drug cartels since 2021 have increasingly used drones to attack the military, police, and rivals. In Ukraine, the extensive use of both off-the-shelf and military drones has further demonstrated drones' lethality and versatility. Drones have even been weaponized here in the U.S. Domestically, the U.S. Secret Service (USSS), since 2018, has encountered hundreds of drones violating temporary flight restrictions that protect the President and others. In January 2022, an animated video released by Iran's leader depicted an Iranian drone targeting a former U.S. President at his home.

- Drones continue to **interfere** with manned aviation, resulting in damage to aircraft, disruptions to airport operations, and economic harm. The Transportation Security Administration (TSA), since 2021, has reported nearly 2,000 drone sightings near U.S. airports, including incursions at major airports nearly every day. The most serious drone incidents force pilots to take evasive action during takeoff and landing to avoid potentially fatal collisions. During 2021-2022, TSA reported 63 drone incidents requiring evasive action, including four involving commercial aircraft. Drones also have collided with helicopters used by the police, first responders, and the military – threatening lives and disrupting missions. Additionally, drones have significantly impacted airport operations. Since 2019, drone incidents have caused U.S. airports to fully halt operations three times, and in 2021, over 30 partial suspensions of operations – resulting in millions of dollars of economic damage.

- Drones continue to disrupt and damage critical infrastructure and services. In the Middle East, drones in 2021 and 2022 have been used to attack international airports and energy facilities, killing or injuring people and halting operations. At home, the energy and chemical sectors consistently report suspicious activity by drones. In 2020, law enforcement discovered a crashed drone outside an electrical substation in Pennsylvania, which had been modified to cause an intentional power disruption. This attempt was unsuccessful, but next time we may not be so fortunate. During 2021-2022, the FBI identified 235 reports of suspicious drone flights at or near chemical plants in Louisiana. Similar UAS incidents also occurred at oil storage facilities in Oklahoma and natural gas facilities in Texas. Particularly in this time of global energy shortages, any interruption of supplies or attack on these facilities could be devastating. In addition to planning or carrying out such an attack, drones may also be used to conduct hostile surveillance or steal U.S. technology.

- Nearly every day, transnational criminal organizations (TCOs) use drones to convey illicit narcotics and contraband across U.S. borders and conduct hostile surveillance of law

enforcement. From August 2021 to May 2022, U.S. Customs and Border Protection (CBP) has detected more than 8,000 illegal cross-border drone flights at the southern border, an average of nearly 900 incursions per month. Since 2019, CBP officers have seized hundreds of pounds of methamphetamine, fentanyl, and other hard narcotics that drug traffickers have attempted to transport through thousands of cross-border drone flights. As drone technology evolves, so does the threat. CBP assesses that TCOs are pursuing the use of larger drones with increased speed, range, and payload capacity – to fly faster, higher, farther and with more contraband – in an effort to evade CBP and law enforcement.

- Drones can be used by hostile foreign intelligence agencies or criminals to collect intelligence and enable espionage, steal sensitive technology and intellectual property, and conduct cyber-attacks against wireless devices or networks. Most commercial drones have high-definition cameras, can be easily retrofitted with a variety of sensors, and are difficult to detect given their small size. Details and data on this aspect of the threat are sensitive and can be best covered in a closed, non-public setting. The potential implications can be significant for sensitive U.S. facilities, the defense industrial base, technology firms, and others.

DHS Uses Current Authority to Detect and Counter Drone Threats, But Gaps Remain

The "Act" grants DHS and DOJ relief from several federal criminal statutes to take certain actions to detect and counter UAS posing a credible threat. Specifically, such relief is largely from provisions of Titles 18 and 49 of the U.S. Code that generally prohibit aircraft sabotage, computer fraud and abuse, interference with the operation of a satellite, wiretapping, and use of pen registers and trap-and-trace devices. This relief allows actions authorized in the Act, including electronic detection and mitigation of UAS threats through communications signal intercept and interruption, kinetic/physical mitigation, and device seizure. This authority expressly enables the protection of a designated "covered facilities or asset"[2] from UAS threats that relate to specific mission sets, which for DHS includes facilities and missions of the USSS protective operations, U.S. Coast Guard (USCG), Federal Protective Service (FPS), and CBP. The Act also authorizes protection of shared DHS and DOJ mission sets, including protection of National Special Security Events (NSSE) (e.g., Presidential Inauguration) and Special Event Assessment Rating events (e.g., Indianapolis 500). Additionally, the shared mission area includes support to state, local, tribal, or territorial (SLTT) law enforcement (upon request of the chief executive officer of the respective state or territory) for mass gatherings that are limited to a specific timeframe and location, within available resources, and also, the protection of an active federal law enforcement investigation, emergency response, or security function that is limited to a specified timeframe and location.

DHS's current authority is essential to critical missions. USSS relies on the authority to protect the President, Vice President, and NSSEs. USCG utilizes the authority to protect sensitive assets, facilities, and special events. FPS uses the authority to protect federal facilities.

[2] Defined in the *Preventing Emerging Threats Act of 2018* 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 an authorized DHS mission, DOJ mission, or joint DHS or DOJ mission, acting together or separately. *See* 6 U.S.C. § 124n(k)(3).

CBP depends on the authority to counter illicit trafficking of narcotics and contraband across our borders and the hostile surveillance of its personnel. Since October 2018, DHS has prudently implemented the C-UAS authority granted through the Act and ensured the protection of privacy, civil rights, and civil liberties. Through over 300 deployments, DHS has proven the safe exercise of C-UAS authority, via extensive coordination with the FAA, and minimized impacts to the national airspace system.

Despite the Act and progress made to date, there remain major gaps in authority that impede DHS's mission to protect national security and public safety. In December 2021, DHS submitted a C-UAS Assessment to this committee and several others in Congress, which evaluated drone threats to U.S. airports and critical infrastructure; current federal or SLTT law enforcement authorities; an assessment of additional authorities needed by each Department and law enforcement; and an assessment of additional research and development needs to counter the threat. The most critical gaps identified by the DHS Assessment include a lack of authority for:

A. TSA to persistently protect U.S. airports – a stunning gap in the Department's authority;
B. SLTT law enforcement to detect and mitigate drone threats; and
C. Critical infrastructure owners and operators to detect drones operating near their facilities or request law enforcement assistance to mitigate drone threats.

The sunset clause in the Act has also made it more difficult to implement new C-UAS programs and initiatives. With no guarantee that the authority would be reauthorized, it has been difficult for DHS to fully prioritize new C-UAS programs, which require long term stability and sustainment. Uncertainty, and competing priorities have exacerbated the situation, leading to challenges with procurement and acquisition, personnel recruitment, and specialized training.

C-UAS Reauthorization Would Fix Major Gaps

DHS strongly supports the Administration's legislative proposal, which represents a comprehensive approach that seeks to reauthorize and expand current federal authority, including for DHS. This legislative proposal is essential for us to continue critical missions to protect national security and public safety while remedying major gaps in authority and policy, so we can keep pace with the dynamic and evolving threat.

1. First, the legislation would reauthorize DHS and DOJ current C-UAS authority. Congressional action is urgently required, as our authority to **take C-UAS actions** will expire in less than three months on October 5, 2022. A lapse in our authority would result in perilous risks and leave the nation vulnerable to drone threats.

2. Second, the legislation would expand authority to remedy gaps identified in the DHS Assessment and during the interagency policy process led by the National Security Council, specifically:

- Authorize TSA to **proactively** protect transportation infrastructure from drone threats, which would remedy an extraordinary gap in the Department's authority.
  - This provision would enable TSA to deploy C-UAS detection and mitigation equipment beyond limited emergency circumstances. TSA has reported an alarming number of drone incursions near airports. Collision with a commercial plane could

endanger lives while disruptions to airport operations would cause significant economic damage to the aviation industry.

- Create a limited 6-year pilot program for SLTT law enforcement to mitigate threats in their jurisdictions through federal sponsorship and oversight by DHS and DOJ.
  - SLTT law enforcement lack the authority to mitigate drone threats; if selected to participate in this pilot, SLTT would have to comply with all federally standardized processes and procedures to include equivalent protections for individuals' privacy and civil rights/liberties.
  - Federal law enforcement and C-UAS equipment are limited and cannot be everywhere. (DHS and DOJ only have been able to protect about 1% of SEAR events.)
  - C-UAS systems would be tested and evaluated by DHS or DOJ and approved by FAA.
  - This measured approach builds on best practices and lessons learned by DHS and DOJ.
  - A select number of SLTT law enforcement agencies would participate in this pilot.
- Explicitly authorize SLTT law enforcement and critical infrastructure owners and operators to conduct drone detection-only with safe and proven technology.
  - Drone detection is critical to air domain awareness. As millions of drones fly in the national airspace, we must distinguish legitimate, compliant operators from threats.
  - Detection equipment authorized for use would be limited to a DHS list of approved systems.
- It is also important to enable critical infrastructure owners and operators to purchase and preposition mitigation equipment, which could be operated by authorized Federal entities or SLTT law enforcement participants in the pilot program.
- All proposed expansions would continue to require safeguards with which DHS and DOJ must continue to comply. These safeguards include: DHS or FAA-approved equipment lists; standard training and certification; risk-based assessments; coordination with FAA to ensure aviation safety; privacy, civil rights, and civil liberties protections; and DHS or DOJ oversight.

How DHS Policy and Guidance Governs the Use of C-UAS Authorities

To ensure consistent application of C-UAS authorities across Components, DHS established a C-UAS Program Management Office (PMO) within the Office of Strategy, Policy, and Plans. The PMO manages and supports C-UAS activities across the Department to ensure Component alignment with the Secretary's strategy and policy guidance and serves as a single point of contact for interagency partners. The PMO has worked closely with the FAA to develop objective standards that define critical elements needed for successful coordination across the Department, in each Component, and for the operator. Additionally, the Secretary issued the DHS-wide C-UAS Policy Guidance on September 10, 2019, requiring DHS Components to establish additional internal C-UAS policies, conduct assessments on the protection of privacy, civil rights, and civil liberties, and develop operational plans for each C-UAS deployment.

How the DHS Process for Authorizing Use of C-UAS Authorities Ensures Oversight

Recognizing the complexity and nuances associated with deploying C-UAS equipment domestically, the DHS Secretary's C-UAS Policy Guidance establishes formal process for obtaining C-UAS deployment authorizations. The process requires all Components to: identify a "covered facility or asset" to be designated; conduct a risk-based assessment prior to requesting the Secretary designate a "covered facility or asset;" coordinate with FAA to allow an assessment of potential impacts to the national airspace system and to evaluate the need and regulatory basis for establishing flight restrictions; and, then obtain authorization from the Secretary to conduct C-UAS activities pursuant to the Act. DHS and FAA closely coordinate these processes to ensure deployments do not negatively impact the national airspace system, to monitor how C-UAS authorities are used, and to ensure senior leadership visibility and concurrence.

How DHS Protects Privacy, Civil Rights, and Civil Liberties When Using C-UAS Authority

DHS is committed to protecting national security, public safety, and our values. These values include respecting the privacy, civil rights, and civil liberties of citizens and visitors, as well as, operating with transparency and accountability. The Secretary designates each covered facility or asset authorized for C-UAS activity. Every request includes an operations plan that clearly defines the boundaries and protocols for that specific protection mission. DHS C-UAS is a limited and controlled program. The only data our C-UAS systems collect are transmissions between the controller and the drone, which are similar to the data that manned aircraft transmits publicly via a transponder. This limited data is collected and retained consistent with the protections of the Act, the First and Fourth Amendments, and guidance from the DHS Privacy Office and the Office for Civil Rights and Civil Liberties. DHS is unable to access other content (e.g., phone calls, texts, email) on the operator's phone or other control device. C-UAS is not a surveillance program.

Above and beyond privacy protections in the Act, DHS applies *Section 222 of the Homeland Security Act of 2002* (as amended) to require DHS Component C-UAS programs to submit a Privacy Threshold Assessment (PTA) and obtain DHS Privacy Office approval prior to deploying C-UAS technology. The DHS Privacy Office uses the PTA to determine the need for a Privacy Impact Assessment (PIA), which includes measures to mitigate privacy risks. Moreover, DHS has published PIAs on its public website. DHS has also issued detailed guidance for collection of communications, data retention and sharing, and considerations on privacy, civil rights, and civil liberties as an annex to the Secretary's C-UAS Policy Guidance.

Again, the Administration's legislative proposal for expansion of C-UAS authorities would map Federal safeguards comparable to those required of DHS and DOJ to SLTT and critical infrastructure owners and operators. These include DHS or FAA approved equipment lists; standard training and certification; risk-based assessments; coordination with FAA to ensure aviation safety is preserved; privacy, civil rights, and civil liberties protections; and DHS or DOJ oversight.

Conclusion

In closing, DHS remains committed to protecting national security and public safety by countering the malicious use of drones. This legislation is essential to continue DHS's critical missions while remedying major gaps in authority, so we can keep pace with the dynamic and evolving threat. We appreciate Congress's foresight in granting C-UAS authority and are ready to work with you and key stakeholders across the government, private sector, law enforcement, and civil society to enact this important legislation. Thank you again for the opportunity to testify today, and I look forward to your questions.