Testimony
of

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

Rear Admiral Scott W. Clendenin
Assistant Commandant for Response Policy
United States Coast Guard
Department of Homeland Security

Austin Gould
Deputy Executive Assistant Administrator (Acting) for Operations Support
Transportation Security Administration
Department of Homeland Security

Dennis J. Michelini
Deputy Executive Assistant Commissioner for Air and Marine Operations
United States Customs and Border Protection
Department of Homeland Security

Regarding a Hearing on
"Assessing the Department of Homeland Security's Efforts
to Counter Unmanned Aircraft Systems"

Before the
United States House of Representatives
Committee on Homeland Security
Subcommittee on Transportation and Maritime Security
and Subcommittee on Oversight, Management, and Accountability

Thursday, March 31, 2022

Chairwoman Watson Coleman, Chairman Correa, Ranking Member Gimenez, Ranking Member Meijer, and distinguished members of the Subcommittees, thank you for inviting us to testify regarding emerging threats posed by the malicious use of unmanned aircraft systems (UAS[1] or "drones"[2]) in the United States and the missions of the Department of Homeland Security (DHS) to counter such threats. DHS continues to judiciously implement the authorities Congress granted through enactment of the *Preventing Emerging Threats Act of 2018* (the "Act"), codified at 6 U.S.C. § 124n, to conduct UAS detection and counter-unmanned aircraft system (C-UAS)[3] activities in response to the evolving and dynamic threat environment, while ensuring the protection of privacy and civil rights and civil liberties. The Department takes implementation of its C-UAS authorities seriously, exercising them to protect national security and public safety while preserving the rights of the public and working with the Federal Aviation Administration (FAA) to minimize impact to the national airspace system (NAS).

Technological advances have accelerated UAS capabilities across a variety of commercial and recreational applications. Their compact size and often low cost make them suitable for many beneficial applications, performing critical tasks with minimal risk and expense. A wide spectrum of domestic users – including industry, private citizens, and Federal, State, local, tribal, and territorial governments – are using or expect to use UAS, which may play a transformative role in fields such as transport and delivery, critical infrastructure management, agriculture, search and rescue, disaster response, public safety, coastal security, military training, and others. Estimates suggest that rapidly advancing UAS technology and integration of drones into the NAS will result in new innovations and generate economic growth and opportunity for businesses and private citizens. DHS supports the lawful use of UAS, including by commercial and recreational users. Like all technology, however, UAS can be exploited for malicious use by threat actors, threatening national security and public safety, which is the major concern of DHS.

Our joint testimony today describes threats to the U.S. Homeland posed by the malicious use of drones and how we use our authorities to protect against these threats. We explain our tiered approach to implementation and governance of C-UAS authorities, including compliance with existing laws and regulations, issuing Department and Component-level policy guidance, and specific privacy, civil rights, and civil liberties documentation that surpasses statutory requirements. Our testimony underscores the processes required to gain Departmental approval and authorization to conduct C-UAS activities, which are designed to protect privacy, civil rights, and civil liberties, safeguard aviation safety, and ensure leadership review of every deployment. Additionally, we will provide examples of DHS Components' C-UAS activities, including testing and operational deployments by the U.S. Coast Guard (USCG), Transportation Security Administration (TSA), and Customs and Border Protection (CBP). Finally, we highlight gaps in the Department's current authorities that sunset on October 5, 2022 – as noted

[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

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

[3] 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. 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.

in the DHS C-UAS Assessment delivered to Congress in December 2021 – and we indicate the Department's intention to request reauthorization and expansion of its C-UAS authorities to remedy such gaps to address dynamic and evolving threats.

Threats to the U.S. Homeland from the Malicious Use of UAS

The malicious use of UAS is increasing and diversifying in the United States and abroad. The threat can take several forms, including kinetic attacks with payloads of firearms, explosives, or weapons of mass destruction; the illicit trafficking of narcotics or contraband; surveillance against law enforcement; cyber-attacks against wireless devices or networks; foreign intelligence; and corporate espionage or theft of intellectual property. The availability of highly capable, low-cost UAS has led to expanded use by threat actors. This has required DHS to grow its domain awareness and response capability efforts to identify and counter smaller, more agile, and less attributable threats across its mission spaces.

We are most concerned with UAS weaponization, smuggling, surveillance, disruption, and the fostering of other illicit activity, particularly in venues where DHS already conducts its missions including airports, border regions, protective operations, National Special Security Events (NSSE), Special Event Assessment Rating (SEAR) events, and mass gatherings. Throughout border regions, CBP personnel have observed UAS used to conduct surveillance and reconnaissance of their operations and have identified a multitude of unmanned aircraft that were deemed as credible threats[4] or enabling other criminal activity such as smuggling, trafficking, and conveyance of illicit materials. At critical infrastructure, key resource sites, sensitive government facilities, and federal properties nationwide, CBP and Federal Protective Service (FPS) personnel have observed UAS operations that appear to conduct intelligence gathering, physical security observation, and strategic reserves assessments on behalf of threat actors. U.S. Secret Service (USSS) officers have identified UAS violating temporary flight restrictions put in place by the FAA to protect the President and other government leaders, the type of threats exemplified by the assassination attempt on Venezuelan President Maduro utilizing explosives-laden drones in 2018. TSA and the Cybersecurity and Infrastructure Security Agency (CISA) continue to engage with transportation sector and critical infrastructure partners to improve stakeholder response capabilities and reaction times to UAS threats.

As we look towards the future, emerging technologies will expand the boundaries of what is possible for threat actors. Capabilities such as controlling multiple drones with one remote, autonomous flight plans, obstacle avoidance, extended communications ranges, and prolonged battery life require constant reevaluation of the Department's prevention and response tactics. Remaining adaptive and proactive in countering UAS threats as they evolve is critical to DHS in executing its missions. Through research, testing, training, and evaluation efforts (RTTE), spearheaded by the DHS Science and Technology (S&T) Directorate, and as recurring

[4] Defined by the Secretary of Homeland Security as, "The reasonable likelihood that a UAS or unmanned aircraft activity, if unabated, would: (i) inflict or otherwise cause physical harm to a person; (ii) inflict or otherwise cause damage or harm to assets, facilities or systems; (iii) interfere with the operational mission, including movement, security, and protection, of a covered facility or asset; (iv) facilitate unlawful activity; (v) conduct unauthorized surveillance or reconnaissance; or (vi) result in unauthorized access to, or disclosure of, classified, sensitive or otherwise lawfully protected information."

innovation and simulation efforts across the interagency mature, we are positioning ourselves to remain ahead of the technology curve.

Current DHS C-UAS Authority and Its Use

The Act grants DHS and the Department of Justice (DOJ) relief from several federal criminal statutes, namely from provisions of Titles 18 and 49 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, to take certain actions to detect and defeat UAS posing 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 designated "covered facilities or assets"[5] from credible UAS threats that relate to specific DHS mission sets, including those covered by CBP, FPS, USCG, and USSS. The Act also authorizes protection of shared DHS and DOJ mission sets including protection of NSSE and SEAR events, a provision for support to State, local, territorial, or tribal 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, and the 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 requirements outlined in the Act and in coordination with the FAA, DHS successfully coordinated 246 operational C-UAS deployments and 30 RTTE events since the authorities were granted. We continue to collaborate closely with the FAA on each deployment to minimize potential impact to the NAS. By partnering with interagency colleagues such as DOJ, Department of Defense (DOD) Joint C-UAS Office (JCO), and North American Aerospace Defense Command (NORAD), our understanding of UAS activity across all domestic environments is maturing, enhancing our ability to differentiate malicious activity from authorized flights, counter credible UAS threats, and share relevant information and data. We see these collaborations and open communication channels as a foundation of shared success to protect the Homeland.

Policy and Guidance Governing DHS's Use of C-UAS Authorities

To ensure consistent application of C-UAS authorities across all Components, DHS established a C-UAS Program Management Office (PMO) within the Office of Strategy, Policy, and Plans (PLCY). The PMO manages and supports C-UAS activities to ensure Component alignment with Departmental strategy and policy guidance and serves as a single point of contact for interagency partners.

---

[5] Defined in the Preventing Emerging Threats Act as any facility 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, or authorized joint DHS or DOJ mission, *See 6 U.S.C. § 124n(k)(3).*

This is especially true for coordination with the FAA. The PMO has worked closely with the FAA to develop an agreed upon set of objective standards that define critical elements of coordination at the Department level, Component level, and operational deployment level. Due to the sensitivities of deploying and operating C-UAS equipment and legal implications associated with relief from provisions of Titles 18 and 49 through the Act, it is imperative to have formal and streamlined C-UAS governance and communication structures in place. Objective standards ensure DHS maintains compliance with existing laws and regulations.

We recognize the critical importance of maintaining the safety and security of the NAS and coordinate with the FAA to develop repeatable processes for safe and efficient deployments of C-UAS technology. The resulting objective standards create consistency across all DHS Components by establishing common definitions, guidelines for conducting risk-based assessments, including coordination with the FAA for assessments of the impact to nearby airport communications and aircraft navigation devices, reporting protocols when C-UAS equipment is "activated" or "transmitting," data retention standards and assessment of the need for other airspace protections, such as flight restrictions.

In addition to these agreed upon objective standards, the Secretary issued the DHS C-UAS Policy Guidance on September 10, 2019 requiring DHS Components to establish their own internal C-UAS policies, conduct assessments to document the protection of privacy, civil rights, and civil liberties, and develop operational plans for each unique C-UAS deployment, among other requirements.

Process for Authorizing the Use of C-UAS Authorities

Recognizing the complexity and nuances associated with deploying C-UAS equipment domestically, the DHS Secretary's C-UAS Policy Guidance establishes formal processes for obtaining C-UAS deployment authorizations. Major process steps include DHS Components identifying a "covered facility or asset" to be designated, coordinating with FAA so they may assess potential impacts to the NAS and evaluate the need and regulatory basis for establishing flight restrictions, and receiving authorization from the Secretary to conduct C-UAS activities pursuant to the Act.

All deployments require Components to conduct a risk-based assessment prior to requesting the statutorily required designation of a "covered facility or asset" from the Secretary. This assessment includes an evaluation of traditional risk elements such as threat, vulnerability, and consequence but also considers collateral risk that C-UAS systems pose to the NAS. DHS provides the FAA with C-UAS equipment operating frequencies so the FAA may evaluate potential interference with nearby airport communications or aircraft avionics (radio frequency spectrum deconfliction). When deconfliction is complete and the FAA has reviewed the operating plan, DHS and the FAA sign a coordination memorandum indicating required coordination steps are complete. The Secretary then designates the requested facility or asset as a "covered facility or asset" and authorizes the Component to take C-UAS actions pursuant to the Act.

DHS and FAA coordinated these processes to enable the FAA to ensure deployments do not negatively impact the NAS, to provide details on how authorities are used, and to ensure

senior leadership visibility and concurrence with operations. We work collaboratively with the FAA to successfully protect a wide range of areas, events, and mass gatherings from UAS threats and continuously review our processes and protocols to streamline tasks where possible.

How Privacy, Civil Rights, and Civil Liberties are Protected During C-UAS Activities

DHS is committed to protecting the security of the Nation and its values. Those values include respecting the civil rights, civil liberties, and personal privacy of its citizens and visitors, as well as conducting operations with openness and accountability.

Understanding how C-UAS equipment works is essential to considering the privacy, civil rights, and civil liberties implications of its use. While drones generally operate on the same frequencies used by publicly available communication networks such as cellular, Bluetooth, and wi-fi, they use an individual network created between the drone and a controller. Some C-UAS equipment DHS uses identifies those communication networks and determines that the link is between a drone and its controller. DHS is unable to access other content on the operator's phone or device if it is being used to control the drone.

In general, the term "mitigation" involves an interruption of the signal from the drone operator's controller to the drone itself. An interruption causes the drone to enter into its pre-programmed recovery protocol, which is often to fly to its pre-designated "home" location or to simply hover in place. In cases where sending a drone "home" does not decrease the threat, some C-UAS equipment emulates a controller, thereby overpowering the signals from the operator's controller and allowing the C-UAS equipment operator to send the drone to a new "home" location or a DHS-preferred render safe location. Of import, C-UAS equipment is *not* constantly transmitting in the radio frequency spectrum; rather, it is generally only transmitting for seconds at a time, and only on the rare occasion when a mitigation action is underway.

The Act includes strong privacy protections. Authorized DHS Components may intercept or acquire command and control (C2) communications to or from a UAS, as an exercise of DHS C-UAS authority, but only to the extent necessary to support C-UAS actions authorized by the Secretary. DHS Components 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 other applicable federal laws and Department policies. In addition to those privacy protections in the Act, the Department 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 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 published multiple C-UAS PIAs for public consumption consistent with requirements outlined in the Homeland Security Act of 2002.

We continue to protect privacy, civil rights, and civil liberties by ensuring that RTTE activities collect only information authorized by law and needed to identify and address UAS threats. Component policies include measures to respect the lawful use of UAS without compromising the protection of a "covered facility or asset." Additionally, we developed procedures and incorporated them into Departmental and Component-level policy guidance and

operational plans to ensure consistency in C-UAS information handling. PLCY issued detailed guidance for developing UAS communication collection, retention, and sharing procedures, as well as addressing privacy, civil rights, and civil liberties considerations to Components as an annex to the DHS Secretary's C-UAS Policy Guidance. These policies are currently undergoing review and revision consistent with lessons learned.

The FAA is a great partner for DHS, supporting the Department's efforts to protect "covered facilities or assets" while preserving access to the airspace for those operating UAS compliantly. When DHS requests temporary flight restrictions (TFRs) to accompany C-UAS activities, the FAA notifies the public of restrictions and provides the means to request a waiver should they have a legitimate need to participate in protected First Amendment activities. Additionally, by collaborating with the FAA to determine if temporary flight restrictions are needed, coordinate waiver requests within the flight restricted area, and issue notices to the public, we ensure those operating UAS compliantly in the area understand the limitations and potential actions that can be taken should they violate airspace restrictions.

Examples of DHS Components' C-UAS Activities, Testing, and Operational Deployments[6]

United States Coast Guard (USCG)

The USCG has safeguarded the American people and promoted national security, border security, and economic prosperity in a complex and evolving threat environment for over 230 years. As the principal federal agency responsible for maritime safety and security in U.S. ports and inland waterways and along more than 95,000 miles of U.S. coastline, the USCG works collaboratively with relevant stakeholders to combat threats to the Homeland and critical infrastructure, and the novel threats posed by UAS are increasingly concerning to USCG leaders.

From 2017 through 2021, the USCG observed a significant increase in suspicious UAS sightings over/near maritime assets and facilities, such as refineries and ferry/cruise ship terminals. Over the same period, UAS interfered with or crashed into USCG assets, ferries, cruise ships, and commercial vessels over 80 times. Since the enactment of the Act, the USCG conducted 26 separate C-UAS events requiring FAA approval, including two NSSEs and five SEAR events.

Currently, there are no flight restrictions over commercial maritime critical infrastructure, and owners and operators at those facilities consistently express their concern about threats posed to facilities by UAS. The USCG views the ability for these critical infrastructure facilities to obtain flight restrictions as an important step in securing the airspace in the maritime and port environments and is working with the FAA to address these concerns.

In preparation for C-UAS operations, the USCG conducts an event specific review of privacy documentation, including any relevant PIAs, to measure the sufficiency of protocols to ensure civil liberties and privacy rights of those individuals affected by C-UAS operations. The USCG also collaborates closely with the FAA so the FAA may assess potential impacts on the

[6] The USSS and FPS have also conducted C-UAS deployments, but those deployments are not summarized in this written testimony.

NAS and the need for a temporary flight restriction and potentially issue public notices advising UAS operators and the public of the location and time period when restrictions are in place.

In addition, the USCG coordinates all C-UAS activities with the FAA, the C-UAS PMO, and other relevant law enforcement stakeholders to ensure appropriate frequency and spectrum management protocols are followed.

Transportation Security Administration (TSA)

Since its creation following the attacks on September 11, 2001, the TSA has dedicated itself to strengthening our nation's transportation systems while ensuring freedom of movement for people and commerce. Drones are one of the latest threats to TSA's mission, and developing ways to deter and prevent potential harm from malicious activity to aviation and other transportation system sectors is one of TSA's top priorities.

In December 2018, reports of UAS sightings close to the runway at London's Gatwick Airport caused the cancellation of 1,000 flights over the Christmas holiday, adversely affecting approximately 140,000 passengers and resulting in severe economic impacts. The UAS operators were never apprehended and the resulting 36 hours of halted commercial air traffic and cascading international aviation system impacts illustrates the significant effects an unauthorized UAS can have on the surrounding airspace. Since the Gatwick incident, the number of UAS sightings reported increased every year, with the TSA receiving almost 1,900 reports of drones operating near airports in 2021, more than double the amount reported in 2020. Already this year, two commercial pilots took evasive action to avoid a drone collision: Air France Flight 007 departing New York for Paris and Sunset Aviation Flight 283 arriving in Atlanta from Orlando.

While TSA's mission is not explicitly called out in the Act, DHS, including TSA, is prepared to protect airports pursuant to the Act's authority to use C-UAS for the protection of an active federal law enforcement investigation, emergency response, or security function, that is limited to a specified timeframe and location. TSA requires every airport Federal Security Director (FSD) to develop and update a Tactical Response Plan (TRP) to support detection, tracking, identification, and in the event of a persistent threat and upon the emergency direction of the Secretary, mitigation of UAS threats at airports. The TRP documents TSA's preparation and response measures to address both errant and malicious UAS activity at and around the airport. FSDs conduct annual C-UAS exercises to test these plans with participation from State, local, tribal, and territorial partners including airport authorities and other federal agencies, such as the FAA and the Federal Bureau of Investigation (FBI).

TSA also established a UAS Threat and Vulnerability Assessments Unit to conduct comprehensive UAS-specific Joint Vulnerability Assessments (JVAs) at airports most at risk from errant or malicious UAS incidents. TSA uses these UAS JVAs to refine TRPs, define site-specific response plans, work with airport authorities and law enforcement partners to improve information sharing procedures, and recommend courses of action for the future. Since February 2021, TSA conducted 17 full UAS-specific JVAs.

Looking to the future, TSA established technology test beds at Miami International Airport and Los Angeles International Airport and is evaluating UAS detection technology for operational effectiveness in the airport environment, in coordination with DHS S&T and the FAA. TSA tests a range of technologies at the sites, including radar, thermal imaging, and electro-optical cameras. TSA uses a continuous technology testing cycle in its UAS test beds to keep up with the rapidly evolving UAS technology market and meet the needs of the interagency, transportation facilities, and industry.

Customs and Border Protection (CBP)

CBP continues to experience high numbers of incidents involving illicit use of unmanned aircraft systems to facilitate unlawful movement of people and narcotics across the southwest border. Transnational Criminal Organizations (TCOs) and possibly Foreign State Actors use UAS to conduct unauthorized surveillance of CBP personnel and operations to pass information to contacts on the ground on where to guide noncitizens or transport illegal drugs to circumvent law enforcement. Sensor records, pilot and agent sightings and other sources of information also indicate the increasing use of drones to transport illegal drugs and other contraband across the border. This illicit activity threatens the safety of our frontline personnel, poses a collision risk to our aircraft, and adversely affects our border security operations.

Over a recent five-month period, CBP sensors captured more than 30,500 drone flights within close proximity of the Southwest Border, of which 4,458 took place during nighttime hours. Additionally, more than 14,000 of these flights exceeded the FAA-regulated altitude of 400 feet, some nearly reaching altitudes of 4,000 feet. Among all these flights, there were only about 4,300 unique drone IDs, indicating that use of drones for illicit cross border activity is not only widespread, but also organized and an integrated element of TCO operations.

The Act has enabled CBP to begin taking responsible C-UAS actions against systems that pose a credible threat to covered facilities or assets along the Southwest border. Consistent with the Act and the DHS Secretary's Policy Guidance, CBP implemented a C-UAS policy and subsequent operations plan in July 2020 after extensive discussion and review to ensure lawful and efficient operational implementation. The overall volume of UAS traffic rapidly expanded in the past few years, and CBP is committed to identifying and targeting illicit activity while protecting lawful commercial and recreational use.

Currently, CBP operates C-UAS devices at select, high-risk locations along the Southwest Border. Operations target specific credible threats and do not involve persistent surveillance of all the border regions. Authorization for CBP C-UAS operations requires a credible threat determination that involves extensive analysis and evidence of the threat, including reports of visual observations and correlation with actionable information and other law enforcement information. All C-UAS operations adhere to authorized statutory and policy parameters to ensure operational integrity and compliance with all legal restrictions and privacy protections.

C-UAS operations are an essential capability to address evolving UAS threats and CBP implemented its risk-based C-UAS approach within a framework that ensures rigorous analysis and clear documentation of a credible threat to identify and target nefarious operators and

devices amongst the increasing amount of drone traffic. Since CBP's implementation of C-UAS operations in July 2020, there were five credible UAS threats mitigated, affirmation of CBP's deliberate, targeted, and diligent application of its C-UAS authority.

C-UAS authorities will become even more critical as the UAS threat evolves. Less than a year ago, the Jalisco New Generation Cartel attacked Mexican law enforcement and a rival cartel with explosives deployed from drones. These incidents, along with indications that TCOs are pursuing the use of larger drones with more maneuverability, more payload capacity, and greater capability – to fly longer, higher, and further – are concerning trends. CBP needs these critical authorities to continue efforts to counter rapidly evolving threats and expand its risk-based implementation of C-UAS operations to additional locations along the Southwest and Northern Borders.

Gaps in Current DHS Authority

On December 21, 2021, DHS submitted the interagency coordinated and statutorily required DHS C-UAS Assessment to evaluate drone threats to domestic critical infrastructure and airports, evaluate current Federal, State, local, territorial, or tribal (SLTT) law enforcement authorities to counter drone threats, and identify additional improvements needed for security. The assessment notes the accelerated technological evolution of drone capabilities across a variety of commercial and recreational applications. As UAS capabilities advance, technologies to detect, identify, monitor, and track UAS must also advance.

The assessment also explains how current legal authorities do not expressly authorize DHS to conduct certain persistent UAS detection and mitigation activities, leaving our Nation's large hub airports and critical infrastructure vulnerable to intentional UAS threats and unintentional hazards. Additionally, the assessment identified gaps in existing authorities that limit the abilities of SLTT law enforcement to effectively deter unauthorized activities, respond to incidents, and enforce laws and regulations. Specific authority for protecting airports and transportation systems combined with a community-based approach to UAS detection would help set both the stage for improved air domain awareness and foundation for threat discrimination and mitigation efforts. These concerns are detailed in the Assessment.

DHS has been working closely with the Administration and interagency partners on a legislative proposal to request reauthorization of our current C-UAS authorities. The Department's approach to reauthorization is grounded in its assessment of the evolving threat landscape as well as addressing key gaps and vulnerabilities that we have identified. We look forward to engaging with you, your staff, and other key stakeholders on those authorities.

Conclusion

DHS is committed to countering the threat of malicious UAS activity facing the Homeland. We are grateful for the continued support of Congress and to our fellow departments and agencies for their support and contributions in this effort. Together we can raise the domestic UAS security baseline, disrupt attacks, and hold accountable those who perpetrate these acts. Thank you again for the opportunity to testify today and we look forward to your questions.