Joint Testimony of

The Honorable David J. Glawe
Under Secretary for Intelligence and Analysis
U.S. Department of Homeland Security

Hayley Chang
Deputy General Counsel
U.S. Department of Homeland Security

Senate Committee on Homeland Security and Governmental Affairs

"S. 2836, the *Preventing Emerging Threats Act of 2018*: Countering Malicious Drones"

Wednesday, June 6, 2018

Chairman Johnson, Ranking Member McCaskill, and distinguished members of the Committee, thank you for inviting DHS to speak with you today. We appreciate the opportunity to discuss the Department of Homeland Security's (DHS) role in countering threats from small Unmanned Aircraft Systems (UAS) in our National Airspace System (NAS).

Introduction

First, we would like to thank the Committee for its attention to this issue and holding this hearing to highlight the critical importance of the interagency efforts to secure the national airspace. We would also specifically thank Chairman Johnson, Ranking Member McCaskill, and the other members of this committee for introducing and cosponsoring a bill that would specifically address our equities in this area – this is a monumental step forward. With enactment of this proposal, Congress would reduce risks to public safety and national security, which will help to accelerate the safe integration of UAS into the NAS and ensure that the United States remains a global leader in UAS innovation.

DHS continues to strongly support the Federal Aviation Administration's (FAA) UAS integration efforts. As the safe integration of commercial and private UAS into the NAS continues, this technology also presents increasing security challenges that require a layered and parallel government security response from federal partners to protect the public from misuse of this technology. The misuse of this technology poses unique security challenges. Generally,

examples of UAS-related threats include recklessly flying UAS near critical infrastructure, intentionally conducting surveillance and counter surveillance of law enforcement, smuggling contraband, or facilitating kinetic attacks on stationary or mobile, and high consequence targets.

We have already seen transnational criminal actors adopt UAS technology to move drugs across the border. Terrorist groups overseas use drones to conduct attacks on the battlefield and continue to plot to use them in terrorist attacks elsewhere. This is a very serious, looming threat that we are currently unprepared to confront. Today we are unable to effectively counter malicious use of drones because we are hampered by federal laws enacted years before UAS technology was available for commercial and consumer use. Public access to these systems, with their current operational capacity and range were not even conceived of when these laws were adopted.

Lack of Authority for Response

DHS is in need of legislative authority to counter the growing threat posed by UAS. Specifically, DHS needs Counter-UAS (CUAS) authorities to detect, track, and mitigate threats from small UAS. Without this mandate, DHS is unable to develop and operate many types of CUAS technologies. If enacted, S. 2836, the Preventing Emerging Threats Act of 2018 will provide DHS the ability to develop the necessary technology and deploy it in support of our identified missions to mitigate the range of threats from small UAS similar to the Administration's CUAS legislative proposal.

The potential misuse of UAS presents unique security challenges. In normal security situations, law enforcement personnel can establish protective measures to protect people and property from mobile threats—that is simply not the case with drones as they are able to access areas that people, cars, or other mobile devices cannot. Moreover, the most effective technologies for countering malicious uses of UAS conflict with federal laws enacted long before UAS technology was available for commercial and consumer use.

DHS and our interagency partners identified significant legal challenges to law enforcement's ability to use the most up-to-date technologies to detect, track, and mitigate the threats from small UAS. Our primary concerns with the existing legal uncertainty fall into three critical areas:

(1) The challenges posed by the rapid technological advancement utilized in UAS;
(2) Strong concerns for our law enforcement personnel subject to potential criminal liability if they were to take action to mitigate a UAS threat; and,
(3) The need to have comparable authority with our Department of Defense (DOD) partners when working together on National Security Special Events, Special Event Assessment Rating events, and other domestic security operations.

As a result, DHS and the Department of Justice (DOJ) need relief from Title 18 to allow us to use the most effective technology to counter the threat posed by UAS and to ensure that our law enforcement personnel are not criminally liable for using this technology. As you are aware, Congress provided DOD and the Department of Energy (DOE) with relief from Title 18 when it provided them with the authority to detect, track, and mitigate the threat posed by UAS in the

FY2017 and FY2018 National Defense Authorization Act (P.L. 114-328 and P. L. 115-91). We are asking that DHS and DOJ be provided the exact same relief from Title 18. This bill, sponsored by Chairman Johnson and cosponsored by Ranking Member McCaskill, Senators Hoven, Heitkamp, Jones, Cotton, Cassidy, and Rubio, is a critical step to our front line officers' efforts to mitigate UAS threats.

Additionally, providing relief from Title 18 will allow DHS to have commensurate authorities with our DOD partners when working together domestically, thus ensuring there are no operational authority conflicts to protect certain facilities, assets, and operations critical to national security against threats from UAS. Moreover, due to the rapidly evolving technology and the uncertainty associated with the application of Title 18 to these technologies, it is key to get relief from statutory barriers that were not originally intended for the UAS context.

If enacted, S. 2836 would authorize DHS and DOJ to conduct limited CUAS operations to identify, track, and mitigate drone threats. These authorities would apply to a narrow set of important and prioritized missions, and it would allow DHS and DOJ to protect Americans and our own personnel who perform law enforcement and protective missions.

The proposed legislation mirrors the existing statutory authority granted to DOD and DOE/NNSA in the 2017 NDAA and the 2018 NDAA (P.L. 114-328 and P. L. 115-91, respectively). DOD and DOE/NNSA have been able to use these authorities to protect designated facilities and assets here in the United States. The bill also contains robust measures designed to protect privacy and civil liberties. Specifically, the proposed bill limits the collection and retention of communications to and from the drone and ensures that such collection is undertaken only for the purpose of mitigating the threat caused by the UAS.

We are grateful for the demonstrated leadership from Chairman Johnson, Ranking Member McCaskill and all of the Senators cosponsoring S.2836 for your efforts to move these needed authorities forward. DHS and DOJ need Title 18 relief which this legislation provides to allow our officers access to technologies to counter the nefarious use of UAS. We cannot stress enough how important this is. The technology associated with UAS has and continues to evolve faster than the legal authorities surrounding it, and it is critical to grant our security operators relief from statutory barriers to ensure the Department can keep pace with evolving threats, adaptive enemies, and emboldened adversaries. DHS will continue to work with Congress to ensure the swift passage of this critical legislation to address the significant threat.

Threat

Since the Department was first authorized in the Homeland Security Act of 2002 (P.L.107–296), DHS has been on the frontlines to secure and protect our Nation. But the world has changed since 2002, in geopolitics, technology, and the threats we face. Today a cellphone has the computing power of the world's fastest supercomputers only twenty years ago. Terrorists now communicate through encrypted cell phone apps and social media and are utilizing sophisticated, commercial technologies to conduct attacks —challenges we couldn't foresee in 2002.

To best protect the United States and its citizens, we need updated authorities, updated support, and updated accountability for the world we live in today. It is time to ensure that the 240,000 DHS employees who work tirelessly to protect the nation have the tools they need to carry out our mission. The capability of small UAS's is quickly evolving and more advanced systems are becoming widely available, making the potential threats even more acute. As these capabilities have become available, DHS has worked aggressively with our interagency partners to keep up with the advancement in technology. This work to increase our capability to counter existing threats and anticipate future ones will never stop – but we can't make it operational without the authority to do so.

Overseas, terrorist groups and criminal organizations use commercially available UAS to drop explosive payloads, deliver harmful substances, and conduct illicit surveillance. Illicit actors, including terrorists, have been working to increase the payload capabilities of UAS for a variety of reasons, which presents a growing challenge of scale in mitigating the immediate effects of potential threats.

Domestically, criminals, including Mexican transnational criminal organizations (TCO), are increasingly using UAS to deliver narcotics across the southern border, conduct illicit surveillance, avoid U.S. law enforcement, and interfere with ongoing law enforcement operations.

But the threat goes even beyond that. Malicious actors could utilize UASs in order to wirelessly exploit access points and unsecured networks and devices. This can include using UASs to inject malware, execute malicious code, and perform man-in-the-middle attacks. UASs can also deliver hardware for exploiting unsecured wireless systems. In 2015, researchers in Singapore attached a smartphone holding applications to a UAS to detect printers with unsecured wireless connections. The researchers flew the UAS outside an office building, had the phone pose as the printer, and tricked nearby computers to connect to the phone instead of the printer. When a user sent a document for printing, the phone intercepted the document and sent a copy to the researchers using a 3G or 4G connection. The document was then sent to the real printer so the user would not know the document had been intercepted.[1]

Malicious actors could also exploit vulnerabilities within UAS and UAS supply chains to compromise UAS belonging to critical infrastructure operators and disrupt or interfere with legitimate UAS operations. Since 2012, a DHS review of publicly available reporting indicates that there has been a notable increase in reporting of UAS activity near or over critical

[1]Zetter, K. (2015). "Hacking Wireless Printers With Phones and Drones." *Wired* www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/. Accessed January 2, 2018.

Cyber Defense Magazine. (2015). "Hacking enterprise wireless printers with a drone or a vacuum cleaner." www.cyberdefensemagainze.com/hacking/enterprise-wireless-printers with-a-drone-or-a-vacuum-cleaner/. Accessed January 2, 2018.

infrastructure; in 2016, over 2,800 incidents were noted in the national airspace, a 44 percent increase over 2015. We expect the trend to continue across all infrastructure sectors.

CBP

A vital component of DHS's ability to monitor operational capabilities, CBP Air and Marine Operations (AMO), Air and Marine Operations Center (AMOC) integrates surveillance capabilities and coordinates national security threat response with other CBP operational components, including U.S. Border Patrol (USBP). It works with other federal and international partners in this effort.[2] AMOC helps AMO and its partners predict, detect, identify, classify, respond to, and resolve suspect aviation and maritime activity in the approaches to U.S. borders, at the borders, and within the interior of the United States. AMOC utilizes extensive law enforcement and intelligence databases, communication networks and the Air and Marine Operations Surveillance System (AMOSS). The AMOSS provides a single display capable of processing up to 700 individual sensor feeds and tracking over 50,000 individual targets simultaneously.

From January 2015 through December 2017, CBP's AMOC documented 59 UAS incidents along the Southwest Border, with Yuma, Arizona, and Brownsville, Texas, being the most prevalent areas for drug smuggling.

USCG

The U.S. maritime domain represents the access point for a majority of commerce, as well as transiting military vessels, hazardous chemical barges, cruise ships, regulated waterfront facilities, and recreational boating. All of these represent potential targets.

The Coast Guard is challenged to conduct its statutory missions over 90,000 square miles of water without the added challenge of UAS interference, either inadvertently or intentionally, with vessels and aircraft. UAS can interfere with many Coast Guard missions, including but not limited to:

- Coast Guard escorts of U.S. Navy high value units (e.g. ballistic missile submarines);
- Coast Guard protection of military outloads and supporting combat operations overseas;
- Active search and rescue operations; and
- Ongoing drug and migrant interdiction.

The Coast Guard is increasingly observing overflights of UAS while performing its missions. In 2017 alone, there were 97 Field Intelligence Reports of known UAS sightings during missions. Recently, a UAS landed on the deck of the Coast Guard Cutter Sea Lion while transiting into San Diego Harbor, a port of strategic military importance to the Nation. The cutter was unable to identify the operator of the device, leaving the crew vulnerable and unable to apply traditional Coast Guard use of force tactics, techniques, or procedures. In March of this year, a Coast Guard

[2] AMOC partners include the Federal Aviation Administration (FAA), the Department of Defense (including the North American Aerospace Defense Command (NORAD)), and the governments of Mexico, Canada, and the Bahamas.

helicopter was forced to take evasive action to avoid a UAS while operating at low altitude. These scenarios are indicative of potential threats our fleet faces daily.

USSS

The Secret Service must be able to secure the airspace surrounding locations where a protectee is, or will be in order to provide the greatest level of security possible. The authority to counter malicious UAS is essential to that mission. The ability of a potential attacker to monitor Secret Service preparations for a protectee visit or to monitor protectee movements from the air would give them information that would facilitate planning a future attack. UAS could be used to not only plan but also conduct an attack on a protectee. Already, the Secret Service has had several instances where special agents and Uniformed Division officers were called upon to respond to UAS observed at or near protected locations. The threat presented by these devices is not hypothetical or in the future. It is here and now. The Secret Service needs all available tools, both technological and legal, to counter the threat posed by malicious UAS.

If enacted, S. 2836 will enhance Secret Service capabilities to secure airspace within the NCR, at sites visited by protectees, and at National Special Security Events. These authorities will enhance UAS early warning systems, which provide protective details with vital information in a timely manner so that they may take proactive measures against unknown UAS threats in order to maintain the integrity of a protective site and secure protectees.

TSA

UAS encounters near major airports remain a growing concern. As part of the FAA airmen certification process, TSA vets all FAA-certificated remote pilot operators against the Terrorist Screening Database. While we are not currently aware of any specific threat reporting targeting our domestic airports or airport operations, in January 2018, press reports indicated adversaries used bomb-laden drones to attack two Russian military bases in Syria. In light of this information, TSA continues to assess the evolving UAS threats to U.S. airports, as well as how those threats may be mitigated in the future, which requires close analysis and coordination with the Federal Aviation Administration.

NPPD/FPS & IP

The Federal Protective Service (FPS) protects more than 9,000 federal facilities across the nation and more than a million people at those facilities each day. Since January 2014, FPS has responded to and investigated 180 UAS incidents. The majority of these incidents have been non-nefarious, although several cases have resulted in criminal charges or other sanctions. Based on this experience, FPS has continuing concern with the following threat and risk vectors:

- Accidental harm or death by out of control drone;
- Unauthorized surveillance of sensitive facilities and operations;
- Disruption of law enforcement activities;
- Disruption of government business/provision of government services to customers;

- Sensor delivery (acoustic, imagery, electromagnetic);
- Contraband/weapons delivery that by-passes security screening; and
- Introduction of chemical/biological/radiological/toxic industrial chemicals into elevated building air intakes.

The Department has been working with critical infrastructure owners and operators to better understand the security risk associated with UAS. In 2018, the National Protection and Programs Directorate (NPPD) formed a joint public-private sector working group under the Critical Infrastructure Partnership Advisory Council framework to better define the risks to critical infrastructure posed by malicious UAS operations. Working group members will consider the effective use of UAS technology to enhance security around the perimeter of a fixed asset and help inform UAS security and resilience priorities. The working group kick-off meeting was conducted in March 2018, in Arlington, VA.

To ensure the working group maintains an active approach, sub-groups will be established to execute various projects, including UAS incident baseline and reporting, nefarious UAS indicators, best practices, and methods for UAS tracking, as well as emergency action plans to address improper use of UASs near a facility or event.

NPPD also informs critical infrastructure owners and operators of the evolving risks associated with UAS through the following resources:

- UAS Website: A website is available for resources on UAS security and response strategies (www.dhs.gov/uas-ci) and a community of interest is maintained on the Homeland Security Information Network (HSIN-CI).
- Countering-UAS Pocket Card: Provides information on current, non-kinetic actions that security and operations officers can take if a UAS is seen near an infrastructure site. It also contains information regarding the different types of UASs and their respective flight ranges and payload capabilities, along with quick tips on how to properly report UAS-related incidents (https://www.dhs.gov/uas-ci).
- Counter-UAS Video Provides information on the threats posed by the nefarious use of UAS, potential implications to critical infrastructure operations, and options for risk mitigation. The video leverages subject matter experts and senior security officials to stress the importance of mitigating the risks associated with this evolving threat (https://www.dhs.gov/uas-ci).

National Capital Region Airspace

Mitigating threats from malicious small UAS operations is a challenge across the entire NAS, but even when the airspace is tightly controlled or heavily restricted, we still face potential threats and are constrained by the same limitations outlined above. One unique challenge is protecting the airspace in the National Capital Region, which is some of the most restricted airspace in the country and is home to the White House, the U.S. Capitol, Congressional office buildings, and a multitude of iconic monuments. This building, your offices, and the safety of millions of visitors to the Capitol Complex are all here. Within this region, the DHS-hosted interagency National Capital Region Coordination Center is the main center for providing coordination across the interagency security enterprise and was created after September 11th to

provide real-time information sharing and tactical coordination to address potential airborne threats. The Center has representatives from the military, the FAA, and certain federal civilian law enforcement agencies on duty at all times to speed communication and coordination in the event of an unknown or hostile airborne track of interest.

Following September 11th, the dimensions of the restricted flight zones over the National Capital Region changed. The FAA implemented the Special Flight Rules Area (SFRA), which includes within its boundaries the Flight Restricted Zone (FRZ) and Prohibited Area 56 (P-56). The White House and the Vice President's residence are located in the P-56. The United States Secret Service is the DHS agency responsible for approving operations within the P-56 and works closely with FAA, Capitol Police, and U.S. Park Police to enable and protect operations in that airspace. In order to enter the SFRA or the FRZ, an aircraft must have approval from the FAA, and the FRZ remains off limits to UAS operators. Despite this layered security approach, we are still experiencing UAS incidents within the NCR that require an appropriate response— even if they are nuisance or non-compliant operators who disregard the rules. The legislation would help DHS provide detection and mitigation capabilities within the NCR to help identify and isolate UAS threats for appropriate mitigation actions.

CUAS Technology / Limitations

Legal uncertainty also impedes the Department's ability to research, develop and test CUAS technologies for eventual CUAS operations by our authorized users. Under current legal constraints, only a very small number of technologies can be employed to detect and track UAS and none can be employed to disable/mitigate UAS in our homeland. Examples of legal CUAS measures include RADAR, electro-optical/infrared, acoustic, and non-transmitting radio frequency sensors. While these technologies will continue to improve, they currently have shortfalls in both range and accuracy, especially in urban settings, and we are still unable to even test those systems due to the current legal restrictions. An example of a currently illegal, but highly effective technology is the ability to access signals being transmitted between a nefarious UAS and its ground controller to accurately geolocate and track both without false alarms, and potentially take over the control of the UAS and/or stop its ground operator without the use of kinetic measures.

While there is a wide variety of commercially available CUAS solutions, most were developed for the military and we have not been able to determine their performance and suitability for homeland security missions due to legal restrictions. This authority will enhance our ability to test and evaluate promising technologies in realistic operating conditions, to guide industries and inform our development of regulations governing their deployment, especially as it relates to potential mitigation measures.

DHS CUAS Mission Space

With approval of this authority, Congress would reduce risks to public safety and national security, which will help to accelerate the safe integration of UAS into the NAS and ensure that the United States remains a global leader in UAS innovation.

We are requesting a narrow grant of authority to protect our highest priority mission space (covered facilities/assets), including:

- Security operations, including securing facilities, aircraft and vessels by the U.S. Coast Guard and CBP;
- Protection operations by the U.S. Secret Service;
- Protection of certain federal facilities by the Federal Protective Service
- Security for Special Events
- Active federal law enforcement investigations, emergency responses, or security operations; and
- Reacting to a known national security threat that could involve unlawful use of a drone.

We also strongly support the additional provision in Chairman Johnson's bill that would allow a state governor or attorney general to request assistance for a mass gathering event that would not otherwise fall into the security for special event category above.

State and local law enforcement are generally responsible for protection of these local events, but neither has authority to use CUAS technologies to counter potential threats. This provision will allow DHS or DOJ to provide assistance, within available resources, when requested by the State Governor or Attorney General. We believe this is an important aspect of our continued coordination with state and local law enforcement partners.

The Administration's proposal, as well as the Chairman's bill, also contains robust measures designed to protect privacy and civil liberties. Specifically, the legislation makes clear that CUAS activities conducted pursuant to the statute will comply with the Fourth Amendment to the Constitution and applicable federal laws. In addition, the proposal limits the collection and retention of communications to and from the drone and only for the purpose of mitigating the threat caused by the UAS. We recognize that deployment of UAS authority could, in certain circumstances, present First Amendment concerns, such as the chilling of protected expression or association. We believe that proper respect for these constitutional limitations can be developed through policy implementing the statutory authority. The DHS Privacy Office and the DHS Office for Civil Rights and Civil Liberties will work with CUAS practitioners, as appropriate, to ensure compliance and oversight of any CUAS activities.

S. 2836 also includes the need for robust coordination and collaborative risk analysis with the FAA to ensure any deployment of CUAS technologies in the NAS is conducted safely and includes fair warning to UAS operators. We have committed to working closely with the FAA to balance our operational security needs with requirements for safe and efficient NAS operations.

Closing

Growth in the UAS market will continue and its adoption for commercial and recreational purposes results in increased UAS encounters over critical infrastructure facilities and large public venues – and those are the non-nefarious actors. UAS technology continues to advance with increased ranges and payload capabilities for a variety of legitimate applications of benefit

to the public – and will continue to evolve toward fully autonomous UAS operations. If we do not want to hinder the positive economic outcome of this technological development, we must advance security measures in parallel.

Although there is no single physical countermeasure to deter or prevent unauthorized UAS encounters, effective deterrence will always include sustained outreach, education, development of safety and training standards, deliberate planning, as well as the integration of technical detection and mitigation capabilities. But right now, we can't test mitigation methods, determine the full scope of the threat, or develop counter measures because of outdated legal restrictions that were not created to cover this issue.

DHS is eager to take the next steps, continue to secure our country against all threats, and prudently act to protect the homeland while respecting privacy and civil liberties. Our dedicated professionals at DHS are on watch 24 hours per day, 365 days per year protecting Americans from threats by land, sea, air, and in cyberspace, while also promoting our Nation's economic prosperity. They take decisive action to protect us all from terrorists, TCOs, rogue nation states, natural disasters, and more. Let us show them we have their backs by working together to secure the authorities and resources they need to do their jobs.

Chairman Johnson, Ranking Member McCaskill, and distinguished Senators of the Committee, thank you again for your attention to this important issue and for the opportunity to discuss our counter UAS efforts.

We look forward to answering your questions.