Department of Justice

STATEMENT OF

BRAD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED

"PROTECTING THE HOMELAND FROM UNMANNED AIRCRAFT SYSTEMS"

PRESENTED

JULY 14, 2022

STATEMENT OF
BRAD WIEGMANN
DEPUTY ASSISTANT ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

BEFORE THE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"PROTECTING THE HOMELAND FROM UNMANNED AIRCRAFT SYSTEMS"

PRESENTED
JULY 14, 2022

Good morning, Chairman Peters, Ranking Member Portman, and distinguished Members of the Committee, and thank you for the opportunity to testify on behalf of the Department of Justice. The Department strongly supports the Administration's consolidated counter-unmanned aircraft systems ("Counter-UAS") legislative proposal. Enacting this legislation is critical to continuing our efforts to protect major national events and important Department facilities and assets from the threat posed by misuse of unmanned aircraft systems ("UAS"), or drones. This bill would also enable us to expand UAS detection and counter-UAS efforts with respect to the types of facilities and assets that the Department can protect, and it would empower our State and local law enforcement partners, subject to appropriate oversight and limitations, to address the threat at events that the federal government does not have the resources to protect, and to protect important State facilities and assets.

I. The Threat Posed by Misuse of Drones

The use of UAS technology in the United States is growing rapidly. UAS will bring substantial benefits to our society and economy as the technology transforms the delivery of goods and the provision of services. In fact, commercial use of drones is already generating billions of dollars of economic growth. Law enforcement and public safety use of drones is also increasing and can enable us to perform critical public safety missions while reducing risk to personnel and the public.

Today there are nearly a million drones in the United States registered with the FAA and doubtless many more that are unregistered. Like other technologies that bring great public benefits, drones present serious risks to the public when misused. In April of this year, the Administration released its "Domestic Counter-UAS National Action Plan," which noted that:

> The UAS threat can take several forms, including platforms designed or modified to conduct kinetic attacks using payloads of firearms, explosives, or possibly even weaponized chemical, biological, or nuclear material; cyber attacks against wireless devices or networks; espionage; and the illicit trafficking of narcotics and contraband.

Beyond use by actors with nefarious intent, UAS are also often employed by operators without knowledge or regard for regulatory boundaries, who create hazards for Federal, state, local, tribal, and territorial governments, commercial activities, and the public.

Four years ago, in a hearing before this committee, the FBI Director testified that "given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering." Although thankfully we have not yet seen a successful drone attack on a mass gathering in the United States, we are starting to see individuals in our country attempting to weaponize drones to conduct attacks against others, just as we have seen occur many times abroad.

In February 2020 a subject was arrested by State law enforcement and charged in connection with his efforts to use a drone to drop explosives near a Georgia mobile home park. In September 2020, a defendant in Pennsylvania was sentenced to five years for his efforts to use an unregistered drone to drop homemade bombs to terrorize his former girlfriend. Not far from the U.S. border, Mexican drug cartels have used drones to drop bombs on their rivals, just as terrorist groups in the Middle East have used them to launch deadly attacks.

Drones can also be misused to disrupt essential government functions. In February 2022, a defendant was sentenced to two years' probation for "buzzing" a group of firefighters in Virginia with a drone multiple times and then crashing the drone into a pole inside the fire station. In September 2019, a defendant in California recklessly operated a drone that crashed into a Los Angeles Police Department helicopter; he subsequently pleaded guilty to unsafe operation of an unmanned aircraft. The drone damaged the police helicopter, forced the pilots into an emergency landing, and damaged a vehicle when the drone fell from the sky after the crash.

We are also seeing an increase in the criminal use of drones in the prison context. In October 2019, a defendant was sentenced to 48 months in prison for operating an unregistered drone to facilitate a controlled substance delivery to the Autry State Prison in Georgia. In the summer of 2021, three defendants, including two brothers, were each sentenced to twelve months in prison for attempting to use a drone to smuggle contraband into the Telfair State Prison in Georgia. Between September 2021 and February 2022, four defendants, including two former federal inmates, pleaded guilty to an elaborate conspiracy to deliver contraband via drones into the federal correctional facility at Fort Dix in New Jersey.

Outdoor mass gatherings, like open-air sports stadiums, are particularly vulnerable to drone attacks. For example, in 2022, a defendant was sentenced after using a drone to drop flyers over spectators at two separate NFL games occurring the same afternoon in California. A more nefarious actor could have used the drone to drop explosives or spray deadly chemical agents on the crowd.

Under the important authority granted in the Preventing Emerging Threats Act of 2018, Congress facilitated certain counter-UAS missions by the Departments of Justice and Homeland Security. The FBI has conducted 70 UAS detection and counter-UAS protection operations at

large events, ranging from the Super Bowl to the New Year's Eve celebration in Times Square. That represents only 0.05% of the over 121,000 events during that time for which State, local, and federal officials requested an assessment and Special Events Assessment Rating so that UAS detection and counter-UAS support could be provided. These numbers make clear that the demand for such support to protect our communities has far outstripped the federal government's limited resources and that we cannot do this alone. The events that FBI has protected have also shown that the threat posed by drones used recklessly, but perhaps not with intent to engage in violence, is significant. During those 70 operations, FBI's counter-UAS teams detected 974 unauthorized drones operating in flight restricted areas, located the operator in 279 instances, and attempted mitigation against 50 drones.

II. The Administration's Consolidated Counter-Unmanned Aircraft Systems Legislative Proposal

Recognizing the growing threat posed by misuse of drones, the National Security Council assembled an interagency group to identify the critical gaps in law and policy that impede our ability to defend our national security interests and public safety from this threat. Based on the work of that group, in April of this year, the Administration released the first-of-its-kind Domestic Counter-UAS National Action Plan ("Action Plan"). That Action Plan identifies a number of gaps and includes eight recommendations to better protect the homeland from those using UAS for nefarious purposes. At the top of the list is a recommendation to "Expand Legislative Exemptions for UAS Detection and C-UAS Mitigation Activities."

The Action Plan's key recommendations are to make the authority in the 2018 Act permanent and to expand it in targeted ways based on our experience under the law and our assessment of the growing threat. The Act's authority will lapse in October 2022 if not extended by Congress. The Administration's consolidated counter-UAS legislative proposal addresses many of those recommendations. The authority remains necessary because use of UAS detection and counter-UAS technology by the Department of Justice and the Department of Homeland Security could otherwise run afoul of various criminal laws that prohibit destructive activity with respect to aircraft as well as interception of signals and communications such as those between a drone controller and a drone. *See, e.g.*, 18 U.S.C. § 32 (the Aircraft Sabotage Act); 18 U.S.C. §§ 2510 *et seq*. (the Wiretap Act, also known as Title III); 18 U.S.C. §§ 3121-3127 (the Pen/Trap Statute). These criminal laws apply even to government conduct, and where they contain exceptions (e.g., for a court to authorize interception of signals), those exceptions are not practical for protective counter-UAS missions in which decisions must be made in real-time to address threats. The exemptions in the 2018 Act do not enable use of UAS detection or counter-UAS technology to permanently protect transportation facilities such as civilian airports; other critical infrastructure such as power plants or oil refineries or chemical facilities; or high-risk prisoner transports. Nor does the 2018 Act permit State and local law enforcement to engage in any UAS detection or counter-UAS activity that require a legal exemption.

Consistent with the Action Plan's recommendations, the consolidated legislative proposal would permanently enact the exemptions that Congress provided to the Department of Justice and the Department of Homeland Security in 2018. It would not require the authority to sunset, which would give us more certainty as we plan for the future. Experience gained over the past

four years has demonstrated both the value of counter-UAS activity by the Departments of Justice and Homeland Security, and that these operations can be conducted safely and with strong safeguards for privacy and civil liberties. Permanent exemptions will enable the Departments of Justice and Homeland Security to invest more resources in this mission with confidence that it will be permitted to continue. The legislative proposal retains the requirements for semi-annual briefings to specified committees, thereby ensuring appropriate Congressional oversight.

The bill would also expand the authority of the Departments of Justice and Homeland Security in important ways to address some of the gaps identified in the Action Plan.

First, the legislation would authorize State, local, Tribal, and territorial ("SLTT") law enforcement entities and owners or operators of airports or critical infrastructure to use certain UAS *detection-only* capabilities, subject to specified conditions and safeguards. As noted above, experience has shown that the demand for protection across the country from UAS-based threats greatly exceeds the federal government's capacity. We need to empower local law enforcement agencies across the country, who are primarily responsible for keeping our citizens safe at the local level, to take the steps needed to protect their communities from this emerging threat. We also need to allow critical infrastructure operators to take steps to protect their own facilities and assets.

Notably, the "detection-only" technology that this part of the bill would authorize would not include authority to mitigate the drone through jamming or to otherwise disrupt drones or other aircraft. Rather, the information obtained through detection of drone signals can disclose the location of the drone operator, so that law enforcement or security personnel can locate that operator and address the threat through more traditional means. The detection technology authorized for use would be tested and evaluated by the Department of Homeland Security or the Department of Justice, and approved by the FAA, the Federal Communications Commission ("FCC"), and the National Telecommunications and Information Administration ("NTIA") to ensure that each system does not adversely impact the national airspace system. Only technologies on the approved list could be employed consistent with the exemptions in the law. Any non-federal entity using detection-only authority must also issue a written policy certifying compliance with the privacy protections in the bill and comply with any additional guidance issued by the Secretary or the Attorney General. This "detection-only" authority would provide significant public safety benefits and could be safely employed today.

Second, the legislation would authorize a limited pilot program for SLTT law enforcement entities, subject to a six-year sunset provision. The Departments of Justice and Homeland Security could designate annually up to 12 SLTT law enforcement entities to engage in *both UAS detection and UAS mitigation* activities, consistent with the safeguards and oversight required in the bill. Those entities would be required to receive appropriate training and vetting to enable them to both detect and mitigate UAS threats to covered facilities or assets, including mass gatherings. Because these operations could include use of more sensitive mitigation technology, all of their activities would have to be coordinated in advance with federal partners including the FAA, which could withhold approval if the FAA identifies a risk to the national airspace system from a proposed operation. Moreover, all activities will be carried

out under the direct oversight of the Departments of Justice or Homeland Security. This is an initial step that will allow Congress, the Executive Branch, and SLTT law enforcement entities to evaluate costs and benefits, learn best practices, and employ transformative technology with controls that will continue to ensure airspace safety and the proper use of the radiofrequency spectrum through required coordination with federal authorities. As with the detection-only authority, SLTT pilot program participants could only use equipment that the Department of Homeland Security maintains on a list of authorized equipment, in coordination with DOJ, FCC, NTIA, and FAA.

Third, the legislation would expressly authorize the U.S. Marshals Service ("USMS") to protect high-risk prisoner transports using UAS detection or mitigation technology. Current authority covers courthouses and prisons but does not expressly address prisoner transports. The bill would close this gap and allow the use of technology where, for example, we believe there is a substantial risk involving a terrorist or organized crime figure whose confederates could use drones to attack or monitor a transport. We estimate that there are fewer than fifty such cases in any year, and even fewer where protection might be provided.

Finally, the legislation and its corresponding policies continue to ensure that we respect privacy and constitutional rights as we conduct our UAS detection and mitigation activities, by limiting government actions towards protected First Amendment activities and restricting what information may be collected and shared. It is important to note that the technologies that we employ typically detect the presence of drones operating in a specific space and the only communications that are identified are the electronic data passed between the operator's controller and the UAS. Those communications direct the physical operation of the drone. The technologies used by the Department of Justice do not extract text messages, e-mail, or internet search histories from phones or tablets used to control drones, nor do they allow law enforcement to listen to voice calls. Specifically, the detection systems collect information such as the drone vendor and model; drone and controlling device serial number and media access control, or MAC, address; geolocation of the drone; location of the controller; and the most recent takeoff location and "home" location. This is much like the information required to be broadcasted by manned aircraft, and similar to that which the FAA will require most drones to broadcast under the Remote Identification of Unmanned Aircraft rule. However, for drones that do not comply with FAA requirements, it is critical that the government can collect the information unilaterally.

As required in the 2018 Act, the Attorney General's Counter-UAS Guidance that regulates Department of Justice component UAS detection and counter-UAS operations contains explicit protections for privacy, civil rights, and civil liberties. These include protections to ensure drones operated by the media are allowed to safely operate within FAA flight restricted areas consistent with FAA regulatory policies and procedures. Department of Justice actions under the law must be consistent with the First and Fourth Amendments, and the Department's Guidance requires each component deploying relevant technologies to train personnel on privacy and civil liberties in the counter-UAS context. Importantly, under the proposed legislation, SLTT entities and owners or operators of airports or critical infrastructure who operate detection technologies would be required to adhere to the same privacy protections imposed on federal law enforcement under the existing 2018 law.

In closing, the proposed legislation by itself will not eliminate the threats presented by malicious or irresponsible use of drones. However, it will significantly enhance our ability to mitigate this threat in a manner that is measured, responsible, and consistent with the FAA mandate to integrate drones safely into the national airspace system.

I appreciate the opportunity to testify today, and I would be pleased to answer your questions.

***