STATEMENT OF ANGELA H. STUBBLEFIELD, DEPUTY ASSOCIATE ADMINISTRATOR FOR SECURITY AND HAZARDOUS MATERIALS SAFETY, FEDERAL AVIATION ADMINISTRATION,
BEFORE THE SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION, SUBCOMMITTEE ON SECURITY
DRONE SECURITY: ENHANCING INNOVATION AND MITIGATING SUPPLY CHAIN RISKS
JUNE 18, 2019

Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee:

Thank you for inviting me to speak with you today. As the Federal Aviation Administration's (FAA) Deputy Associate Administrator for the Office of Security and Hazardous Materials Safety, I share the Associate Administrator's responsibilities for formulating policies and plans, and directing national programs involving internal security, intelligence analysis and threat warning, emergency response, and safe air transportation of dangerous goods. This includes ensuring programs and operations are coordinated and integrated with the appropriate external and internal organizations. My office coordinates regularly with the National Security Council (NSC), the Departments of Defense (DOD), Homeland Security (DHS), Justice (DOJ), and Energy (DOE), as well as other security and safety partner agencies at the federal, state, and local levels, to resolve complex national security, safety, and crisis-response challenges. My office is helping to coordinate FAA engagement with stakeholders on Unmanned Aircraft System (UAS) security issues including UAS detection and Counter-UAS (C-UAS) policy.

UAS technology represents one of the fastest growing sectors in aviation today. The volume of UAS operations is outpacing manned aircraft, and there are currently nearly four times as many UAS as registered manned aircraft. UAS are used every day to inspect infrastructure, provide emergency response support, survey agriculture, conduct geological and environmental surveys, and to go places that are otherwise dangerous for people or other

vehicles. Entrepreneurs around the world are exploring innovative ways to use UAS in their commercial activities. The need for us to fully integrate this technology into the National Airspace System (NAS) in a safe, secure, and efficient manner continues to be a national priority—one in which both the FAA and our security partners are heavily invested.

UAS technology offers tremendous benefits to our economy and society, as Congress has recognized, but we must also acknowledge that potential misuse of this technology poses unique security challenges that enable bad actors to overcome the traditional ground-based security measures in place at most sensitive facilities. Today, I would like to discuss with you the FAA's efforts in support of the safe, secure, and efficient integration of UAS into the NAS, including the status of our work with our federal partners to implement counter-UAS authorities and coordination efforts with airport sponsors and other critical infrastructure owners to support their desire to identify and respond effectively to the safety or security risks that may be posed by the errant or malicious use of UAS.

Safe and Secure Integration of UAS into the NAS

The FAA's primary mission is to provide the safest, most efficient airspace system in the world. The FAA uses its statutory authority to carry out this mission by issuing and enforcing regulations and standards for the safe operation of aircraft, by developing procedures to ensure the safe movement of aircraft through the nation's skies, and by providing air traffic control and other air navigation services. In exercising its authority, the FAA also must consider the public's right of free transit through the navigable airspace. This requires close coordination to balance the needs of our security partners with the right of airspace access for both manned and unmanned aircraft. Consistent with our mission, in 2016, the FAA issued the basic rules for

small UAS operations—14 C.F.R. part 107—which set the global standard for integration and provided small UAS operators with unprecedented access to the NAS.

Recently, as part of our effort to address the ever-expanding universe of UAS operations and capabilities, the FAA together with the Department's Office of the Secretary published a proposed new rule on the operation of small UAS over people.[1] The proposal seeks to balance the need to mitigate safety risks with supporting technological and operational advances. The FAA also recently published an advanced notice of proposed rulemaking seeking public input to identify UAS safety and security issues and explore ways to mitigate risks UAS may pose to other aircraft, to people on the ground, or to national security.[2] The FAA's security partners have highlighted for us some of the important security and public safety questions as we work through these issues. Further, in February 2019, the FAA published an interim final rule on external marking requirements for small UAS.[3] The rule requires small unmanned aircraft owners to display their unique identifier (FAA registration number) on an external surface of the aircraft. Small unmanned aircraft owners are no longer permitted to enclose the FAA-issued registration number in a compartment. The FAA took this action to address concerns expressed by the law enforcement community and the FAA's interagency security partners regarding the risk a concealed explosive device poses to first responders who must open a compartment to attempt to find the small unmanned aircraft's registration number.

I would also highlight the work of our joint industry Unmanned Aircraft Safety Team (UAST), which is taking a data-driven approach to the analysis of small UAS safety issues and

[1] https://www.federalregister.gov/documents/2019/02/13/2019-00732/operation-of-small-unmanned-aircraft-systems-over-people

[2] https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems

[3] https://www.federalregister.gov/documents/2019/02/13/2019-00765/external-marking-requirement-for-small-unmanned-aircraft

potential mitigation initiatives. This joint government - industry collaboration is a key effort by FAA's UAS Integration Office and engages leaders from government and a wide variety of industry participants.

Going forward, however, perhaps one of the most important UAS efforts underway at FAA is drafting a remote identification rule. The ability to remotely identify UAS operators and connect them with a UAS in flight will be a crucial stepping stone for UAS traffic management and will facilitate what we envision as high volume, safe, and secure low-altitude UAS operations. Congress recognized the importance of remote identification when it enacted the FAA Extension, Safety, and Security Act of 2016. That Act laid the foundation for the FAA's work with operators and our security partners to realize the importance of remote identification and to reach a consensus on how to address it. More recently, the FAA Reauthorization Act of 2018 provided the FAA with additional authority to move ahead with work on universal registration and remote identification—both of which are critical to the success of commercial UAS operations and safe and secure UAS integration more broadly.

Remote identification is fundamental to both safety and security of UAS operations. Remote identification will be necessary for routine beyond visual line-of-sight operations and operations over people, package delivery, operations in congested airspace, and for the continued safe operation of all aircraft in shared airspace. It will also be foundational for the advancement of automated passenger or cargo-carrying air transportation—what is often referred to as Urban Air Mobility. From a security perspective, remote identification is vital to enabling us to connect a suspect UAS to its control station location and to identify the registered owner of a suspect UAS. With universal remote identification, the FAA, our national security partners, and state and local law enforcement will be better able to locate and identify a UAS operator, determine if

a UAS is being operated in an unsafe, unauthorized, or criminal manner, and take appropriate action if necessary. The FAA is committed to establishing remote identification requirements as quickly as possible.

Congress has recognized that integration of UAS into the NAS will require dedicated traffic management. In 2016, Congress granted authority to the National Aeronautics and Space Administration and the FAA to conduct research and a pilot program for Unmanned Aircraft Systems Traffic Management (UTM). UTM is essentially a set of concepts and tools being developed to safely de-conflict and facilitate dense low-altitude UAS operations. In 2018, Congress provided continued broad authority for UTM implementation, which will allow the FAA to continue its important work to balance the needs of all system users and ensure that UAS are safely and securely integrated into the NAS. DOD, DHS and other national security partners have joined in the development of UTM concepts to support their missions. The FAA is already implementing prototype foundational UTM capabilities such as the Low Altitude Authorization and Notification Capability (LAANC), which gives UAS operators the ability to request and receive near real-time response from the FAA to authorize operators to quickly plan and execute their flights in controlled airspace.

We are also using our existing airspace authority to address concerns about unauthorized UAS operations over certain national security-sensitive federal facilities. To date, we have restricted UAS flights over military installations and vessels, sensitive energy facilities, and iconic landmarks, like the Statue of Liberty, Hoover Dam, and Mount Rushmore, in the interest of national security. To ensure the public is aware of these restricted locations, we created on the FAA website an interactive map and repository of geospatial data used by UAS Service Suppliers and others, and we have updated our B4UFLY mobile app to include a warning to

users in close proximity to these sites. This work is also informing our efforts to determine the most efficient and effective way to implement section 2209 of the FAA Extension, Safety, and Security Act of 2016, which will establish a process for critical infrastructure owners to petition the FAA for UAS-specific flight restrictions over their facilities.

Counter-UAS Authority

Through the Fiscal Year 2017 and 2018 enactments of the annual National Defense Authorization Act, Congress provided DOD and the DOE with authority to respond to UAS that pose a threat to designated facilities and assets. To ensure that C-UAS systems are operated safely in the NAS, Congress requires close FAA coordination with DOD and DOE to define what actions constitute a credible threat, develop a concept of operations for employing C-UAS systems, analyze and mitigate the spectrum impact of selected systems, and draft notification procedures and reporting requirements. Pursuant to similar authority contained in the FAA Reauthorization Act of 2018, DOJ and DHS are also working closely with the FAA to ensure that UAS detection and mitigation technologies are tested, evaluated, and deployed in a manner that minimizes adverse impacts on airspace access, air navigation services, avionics, and other systems that ensure safe and efficient operations in the NAS, while also protecting individuals' privacy and civil liberties.

The FAA's role in supporting our partner agencies' research and eventual use of C-UAS technologies is to ensure that the safety and overall efficiency of the NAS is not compromised while facilitating their security responses. The FAA must be involved in deployment of C-UAS technology at each fixed location, and for *ad hoc* and mobile operations. We must conduct specific, data intensive analyses for each potential deployment of C-UAS to ensure the concept of operations balances the need for operator notification, airspace access, and appropriate

airspace safety mitigations with the protective missions of our security partners. Neither the FAA nor our partner agencies want to jeopardize aviation safety or interfere with compliant UAS operations. In order to strike that balance, the FAA will continue working closely with all of our partner agencies as they deploy C-UAS technology at sensitive facilities and to cover high-risk operations and assets in the United States. We worked through many of the toughest aspects of C-UAS deployment with DOD and DOE and are now sharing these processes and procedures with DHS and DOJ in order to expedite their implementation.

C-UAS in the Airport Environment

Section 2206 of the FAA Extension Safety, and Security Act of 2016 required the FAA, working with DHS and other relevant federal agencies, to evaluate UAS detection technology at airports. From February 2016 through December 2017, the FAA and our partner agencies observed and assessed UAS detection technologies operating at domestic airports in Atlantic City, New York City, Denver, and Dallas-Fort Worth. Through this important work, the FAA learned that the airport environment presents several unique challenges to the effective use of such technologies. The technical readiness of the systems, available at the time, combined with a multitude of other factors, such as geography, interference, location of the majority of reported unauthorized UAS sightings, and the cost of deployment and operation, demonstrate that more testing, evaluation, technology development, and sensor integration is required for effective use in domestic civil airport environments.

In view of these results, the FAA believes other actions, such as education and outreach in the local community, as well as implementation of remote identification requirements, offer effective and cost-efficient options to address many of the concerns related to non-compliant UAS operations on and around airports and air traffic patterns. That said, with the December

2018 protracted UAS disruption at Gatwick Airport, and other disruptions at airports around the world and in the United States, we understand and share the concerns of airport sponsors and our security partners regarding the potential safety hazards and security threats presented by errant or malicious UAS in the airport environment. A number of airport sponsors have acquired or are pursuing possible acquisition of UAS detection systems for their airports. In an effort to make sure such activity is conducted in a safe and coordinated manner, in early May, the FAA sent informational correspondence to airport sponsors, which included information to support informed airport decision-making regarding the potential issues surrounding the demonstration or installation of UAS detection systems at airports (including the legal uncertainties posed by certain UAS detection systems), answers to some frequently asked questions, and technical considerations that the FAA has used to assess the readiness of UAS detection technologies.[4] The FAA wants to coordinate with airports that plan to use UAS detection systems to ensure deployment and use does not create interference or obstruction with aviation safety and efficiency systems at the airport.

Another serious consideration is the quality and timeliness of data provided from privately developed and purchased detection systems. Poor quality information could lead to a reaction that is more detrimental than the errant UAS itself. Such information could cause a significant distraction to air traffic control and create unnecessary delays. Detection systems would be a tool for airports to determine if there is in fact a UAS in their airspace. That detection is the first step in determining whether a UAS poses a threat. This underscores the importance of implementing remote identification. Remote identification will provide critical information to help determine the errant UAS operator's intent. In addition, it is imperative that airports

[4] https://www.faa.gov/airports/airport_safety/media/Updated-Information-UAS-Detection-Countermeasures-Technology-Airports-20190507.pdf

develop and coordinate risk-based operational response plans with relevant airport stakeholders, including the FAA, the Transportation Security Administration, and airport law enforcement, to ensure safety hazards or disproportionate efficiency impacts are not created when attempting to respond to a potential security risk.

In the FAA's May communication with airport sponsors, the Agency also reiterated its objection to the use of UAS mitigation systems by any public or private sector entity outside the four federal Departments that have been provided statutory authority for C-UAS. Given the impacts many UAS mitigation technologies can have on the safety and efficiency of manned aircraft operations, compliant unmanned aircraft, and the provision of air navigation services, the FAA does not currently endorse the general use of any UAS mitigation technology on or around an airport. The use of mitigation technology could introduce more disruption and safety risk than the suspect UAS operation, the very thing its use is intended to counter.

However, given the events in Gatwick, there is no doubt about the significant operational and economic impacts a persistent UAS disruption can have in the airport environment and the need to be able to not only detect, identify, and track a disruptive UAS but also to be able to take action to end the disruption. The FAA along with our federal security partners have formulated a concept of operations (CONOPS) for a National Federal Response plan through which current federal C-UAS authorities and existing federal C-UAS equipment can be rapidly projected into a major U.S. airport experiencing a persistent operational disruption due to an unauthorized UAS operation. This CONOPS has been socialized with airport and airline associations and should be finalized for implementation soon.

While there are a number of UAS detection and mitigation technologies in the marketplace, relatively limited testing and evaluation of these systems has been conducted at

airports and in other domestic civil environments due in large part to legal constraints. The efficacy of their performance and the collateral impacts of their use have not been documented sufficiently to provide confidence in their purchase or use. The 2018 FAA Reauthorization Act directed the FAA to undertake several pilot program activities related to testing and evaluation of UAS detection and mitigation technology, including at airports (Section 383) and to support safety enforcement (Section 372). In addition, the FAA was directed to establish standards for the use of C-UAS systems and to develop a plan for permitting, authorizing, or allowing the use of such systems in the NAS (Section 383). The Agency is currently developing plans and milestones for these efforts.

Enforcement

The interagency work to address the security challenges presented by UAS appropriately has been focused on the risks presented by criminal operations. To date, however, the FAA and our security partners assess that a preponderance of the non-compliant UAS operations that have occurred are likely errant with no malicious intent. These errant operations present a safety concern, which the FAA is addressing in a number of ways. First, public education and outreach are key to reducing these incidents. Efforts such as the "Know Before You Fly" information campaign and the small UAS registration process serve as opportunities to help UAS operators understand the rules and responsibilities for flying an aircraft in the NAS. The Agency is also working to implement the requirements of Section 349 of the 2018 FAA Reauthorization Act, which, among other things, provided the FAA with authority to require knowledge testing of recreational users. Section 349 also requires recreational flyers to receive authorization from the FAA to fly in controlled airspace and provides better clarity on authorized operations. In the

future, the FAA anticipates opening the LAANC system to recreational pilots to allow users the ability to efficiently request and receive authorization to operate in controlled airspace.

That said, if an operator is unwilling or unable to comply with applicable regulations, or is deliberately flouting the regulations, the FAA will not hesitate to take enforcement action. We have a range of civil enforcement tools available to address a violation of federal regulations—from warning letters to civil penalties, and, in the case of an FAA certificate holder, suspension or revocation of that certificate. Civil penalties range from a maximum per violation penalty of $1,466 for individual operators to $32,666 for large companies. Congress also gave the FAA authority to assess civil penalties of up to $20,408 for interfering with law enforcement, first responders, or wildfire fighting operations. The FAA may take enforcement action against anyone who conducts an unauthorized UAS operation or who operates a UAS in a way that endangers the safety of the NAS. Since the promulgation of 14 CFR part 107 (August 2016), the FAA has initiated more than 35 legal enforcement actions for unauthorized UAS operations

The FAA also supports criminal investigation and enforcement actions by federal, state, local, tribal and territorial law enforcement agencies through its Law Enforcement Assistance Program (LEAP) and as part of its airspace security planning for sensitive events such as this year's Super Bowl. LEAP special agents and the FAA's operations security personnel engage in extensive outreach and education efforts that include providing guidance on the FAA's website to assist the law enforcement community in responding to UAS incidents and hosting monthly UAS information webinars. Law enforcement officials are often in the best position to detect and deter unsafe and unauthorized UAS operations, and we rely heavily on their reports to provide us with actionable information concerning these incidents. Accordingly, the FAA works closely with these agencies to develop and implement airspace security plans to protect sensitive

events, provide them with investigative support and information, as well as to provide a communications link where these law enforcement agencies can pass along reports and receive assistance in a timely manner.

Cyber and Data Security Risks

While security risks posed *by* the malicious use of UAS are usually the focus of our discussions with critical infrastructure owners and security partners, increasingly there are concerns about threats *to* the safe and secure use of UAS due to cyber and data security risks. The FAA considers cyber and data security risks and mitigations in every aspect of our mission, including as they apply to aircraft certification and systems as well as to protection of our own air navigation services infrastructure. As FAA does with manned aviation, the Agency takes a risk based approach regarding system and data protection for UAS. While UAS are aircraft, they are also like so many highly computerized devices we use in our professional and personal lives. They can collect data and connect to the internet where information systems and data can be vulnerable to misuse if they are not adequately protected. UAS operators, like computer users, need to be aware of what data is on their systems and consider what level of protection is required. The FAA strongly recommends that UAS operators read the user licensing agreements for their UAS and consider whether the data access, sharing, and protection policies the manufacturer has in place are adequate or whether their data sensitivity necessitates additional protection from disclosure and misuse. The FAA is also looking at agreements the Agency has with non-federal UAS service suppliers to ensure data transparency, sovereignty, and protection requirements are included. Lastly, the FAA continues to work with its federal national security partners to identify and address cyber and data security threats to aviation generally, including those specifically related to UAS.

Conclusion

A robust security framework is critical to advancing the Administration's goal to fully integrate UAS into the NAS. By enabling federal security and federal law enforcement agencies to detect and mitigate UAS threats and risks posed by errant or malicious UAS operations, and by working with operators to develop the technology to help minimize the risks posed by UAS, the United States will continue to lead the way in UAS innovation, and offer the safest and most efficient aviation system in the world. Working together, we are confident we can balance safety and security with innovation. We thank the Committee for its leadership on this issue, and we look forward to working with you as we continue to safely, securely, and efficiently integrate UAS into the NAS and solidify America's role as the global leader in aviation.

This concludes my statement. I will be happy to answer your questions at this time.