STATEMENT OF ANGELA H. STUBBLEFIELD, DEPUTY ASSOCIATE ADMINISTRATOR FOR SECURITY AND HAZARDOUS MATERIALS SAFETY, FEDERAL AVIATION ADMINISTRATION, BEFORE THE SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE, "S. 2836, THE PREVENTING EMERGING THREATS ACT OF 2018: COUNTERING MALICIOUS DRONES," JUNE 6, 2018.

Chairman Johnson, Ranking Member McCaskill, Members of the Committee:

Thank you for inviting me to speak with you today. My name is Angela Stubblefield, and I am the Deputy Associate Administrator for the Federal Aviation Administration's (FAA) Office of Security and Hazardous Materials Safety. In this role, 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, including the National Security Council (NSC), the Departments of Defense (DOD), Homeland Security (DHS), Justice (DOJ), and our other security and safety partner agencies, to resolve complex national security, safety, and crisis-response challenges. My office has become the focal point within FAA for coordinating Unmanned Aircraft System (UAS) security issues and Counter UAS (C-UAS) policy.

UAS technology represents the fastest growing sector in aviation today. UAS, more commonly referred to as drones, are being used every day to inspect infrastructure, provide emergency response support, survey agriculture, and to go places that are otherwise dangerous for people or other vehicles. Entrepreneurs around the world are exploring innovative ways to use drones in their commercial activities. As of May 21, 2018, the FAA has processed over 1 million UAS registrations. The need for us to fully integrate this technology into the National

Airspace System (NAS) in a safe and secure 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 role in maintaining the safety and efficiency of the NAS, the status of our interagency work with our federal partners to address security challenges posed by UAS, and the next steps in building a robust security framework to support the full integration of this technology into our aviation system.

FAA's Mission is to Ensure the Safe and Efficient Use of the NAS

The FAA's primary mission is to provide the safest, most efficient airspace system in the world. We are responsible for providing air traffic control and other air navigation services 24 hours a day, 365 days a year, for 29.4 million square miles of airspace. In addition to this critical operational role, the FAA uses its statutory authority to carry out this mission by issuing and enforcing regulations and standards for the safe operation of aircraft, and by developing procedures to ensure the safe movement of aircraft through the nation's skies. 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.

Safety of Small UAS Operations

Consistent with our mission, in 2016, 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 drone operators with unprecedented access to the NAS. The provisions of part 107 are designed to minimize risks to other aircraft, people, and property on the ground. Among other things, the regulations require pilots to keep an unmanned aircraft within visual line-of-sight, and to operate only during daylight, unless the drone has anti-collision lights, which enable twilight use. The regulations also address altitude and speed restrictions, as well as other operational limits, such as prohibiting flights over unprotected people on the ground who are not directly participating in the UAS operation.

Part 107 also creates a new pilot certificate—the Remote Pilot Certificate—which is designed to ensure that a person operating a small UAS has the basic level of knowledge required to safely fly an unmanned aircraft in the NAS. The Transportation Security Administration recurrently vets all FAA certificate holders, including those who hold Remote Pilot Certificates. Additionally, part 107 creates airspace rules specific to small UAS operations. Part 107 allows operation in uncontrolled Class G airspace without the need for approval from the FAA. Operations in controlled airspace—Class B, C, D, and surface area E—require prior approval from air traffic control.

Airspace Management

One of the biggest challenges for our federal security partners is threat discrimination—knowing who is flying where helps the FAA and our security partners understand what the operator's intent may be, and is critical to threat assessment and response. In addition to the inherent safety benefits of knowing the location of an unmanned aircraft, remote identification of UAS will provide more accurate and critical data that will allow direct and immediate contact with a UAS operator, education of the operator, or, when necessary, enforcement action against the operator to address a violation of federal regulations. We, along with our security and law

enforcement partners, need to be able to quickly identify unmanned aircraft and their operators in order to discern between the clueless, the careless, and the criminal—including serious threats to national security—and to ensure that all operators conduct compliant operations or face the consequences of introducing a safety or security risk into the NAS.

Compliance with basic airspace requirements—the "rules of the road"—is essential to maintaining safety in the NAS and ultimately will make it easier for our national security and law enforcement partners to recognize a drone that is being operated in an unsafe or suspicious manner. To facilitate airspace approvals for small UAS operators, last November, we deployed the prototype Low Altitude Authorization and Notification Capability (LAANC) at several air traffic facilities to evaluate the feasibility of a fully automated solution enabled by public/private data sharing. Based on the prototype's success, we began the first phase of a nationwide beta test of LAANC on April 30, 2018, enabling LAANC services at about 80 airports. This rollout will continue incrementally to nearly 300 air traffic facilities covering approximately 500 airports. We expect to complete nationwide deployment in September 2018.

LAANC uses airspace data based on the FAA's UAS facility maps, which show the maximum altitudes in one square mile areas around airports where UAS may operate safely under part 107. It gives drone operators the ability to request and receive real-time authorization from the FAA, allowing them to quickly plan and execute their flights. LAANC also makes air traffic controllers aware of the locations where planned drone operations will take place, and it can provide information on aircraft that have requested access to a defined airspace.

LAANC is an important step toward implementing UAS Traffic Management (UTM). We view UTM as a suite of capabilities that will incorporate components from the FAA, industry, and our government partners to create a comprehensive system of low-altitude airspace

management for UAS. Our plan for future UTM capabilities includes a number of components—LAANC, remote identification, and dynamic airspace management—that will support the needs of industry, FAA, and our security partners.

Ultimately, UTM will enable UAS operations beyond visual-line-of sight to become routine. As UAS capabilities and their use increase, however, so too does the level of concern among the security and defense communities. DOT and FAA have been working closely with our security partners to better understand these concerns, communicate them to our industry partners, and move forward with opportunities to advance UAS integration while addressing and mitigating security risks.

We are using our existing airspace authority to address concerns about unauthorized drone operations over certain national security-sensitive federal facilities. To date, we have restricted drone flights over military installations, sensitive energy facilities, and iconic landmarks like the Statue of Liberty, Hoover Dam, and Mount Rushmore in the interest of national security. We are also working on additional federal agency requests for restrictions for Federal Bureau of Prisons and U.S. Coast Guard facilities. To ensure the public is aware of these restricted locations, we created an interactive map available on the FAA website, 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.

Interagency Coordination

Coordination and collaboration with our national defense, homeland security, and law enforcement partners is not new to the FAA. We have been working together successfully to address security risks concerning manned aircraft for decades, such as providing air traffic control support for Operation Noble Eagle, and implementing temporary flight restrictions in support of presidential movements and incident response. Our collaboration with security partners to address the challenges presented by unmanned aircraft is a natural extension of this relationship. We have been able to utilize existing processes, procedures, and lessons learned in working together to improve our ability to assess and respond to threats posed by the malicious use of UAS. However, given the unique security risks presented by malicious UAS, more must be done if we are to realize the benefits of full safe and secure integration of UAS into the NAS.

Drones have been used for illegal, malicious purposes both domestically and internationally. Compared to manned aircraft, drones are widely available and have a significantly lower purchase price. They require minimal training, can be operated from almost anywhere, and offer the capacity to bypass traditional, ground-based security measures. They are also generally difficult, if not impossible, to detect using conventional surveillance technologies like radar. Most also currently lack the on-board equipment typically used by manned aircraft for in-flight identification. These characteristics make UAS an attractive option for terrorists and criminals. Examples of the security threats faced by our federal security and defense partners include: kinetic attacks against high-profile people and locations; the delivery of contraband, such as narcotics, across borders and into correctional facilities; surveillance of critical infrastructure and other sensitive national security sites; cyber crimes; and disruption of law enforcement and emergency response operations.

As Congress recognized in the 2016 FAA Extension, significant legal, policy, and technical challenges exist in countering threats posed by the malicious or errant use of drones. The statute clearly articulates Congress's acknowledgement that these security challenges require a layered and integrated government response. We continue to work with our federal partners to develop policies and procedures that will support protection of critical facilities and assets from UAS-based threats, while increasing regulatory compliance and preserving airspace access and the safety and efficiency of operations in the NAS.

Counter UAS (C-UAS) Authority

Congress has provided the DOD and the Department of Energy (DOE) authorities to respond to UAS that pose a threat to designated facilities and assets. FAA has been working in close coordination with DOD and DOE on implementation of these authorities in order to ensure that C-UAS systems are operated safely in the NAS. FAA has worked with DOD and DOE to define what actions constitute a threat, develop a concept of operations for employing C-UAS systems at fixed sites, analyze and mitigate the spectrum impact of selected systems, and draft notification procedures and reporting requirements.

Unlike DOD and DOE, most federal departments and agencies do not have the necessary authority to use some of the most readily available technologies to protect sensitive facilities, operations, and people from the malicious or errant use of UAS due to constraints imposed by federal law. Due in part to potential conflicts with certain federal laws, public and private entities have limited authority to deploy technologies that can detect, track, identify, and, when necessary, mitigate UAS that pose a security threat.

Legislative Proposal for Additional C-UAS Authorities

Recently, the Administration released a legislative proposal to enable DOJ and DHS to protect certain facilities, assets, and operations critical to national security, against threats from UAS. The DOT and FAA were heavily involved in developing and supporting the Administration's proposal, which includes relief from Title 18 restrictions. Under this proposal, DOJ and DHS will work closely with FAA to ensure that detection and mitigation technologies are tested, evaluated, and deployed in a manner that minimizes adverse impacts on airspace access, as well as air navigation services, avionics, and other systems that ensure safe and efficient operations in the NAS.

DOT and FAA support the Administration's phased approach to seeking C-UAS authorities, and the mirroring of the requirements and mechanisms established in the FY 17 and FY 18 National Defense Authorization Acts (NDAA) in the Administration's legislative proposal. Many of the currently-available UAS detection, tracking, and mitigation systems utilize radio-frequency based technologies that could interfere with the aviation spectrum, negatively impacting air navigation service and avionics systems critical to the safety of flight. Therefore, extensive coordination before, during, and after deployment is required, and safety impacts must be mitigated, in order to safely deploy these technologies in the NAS.

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. FAA must be involved in deployment of C-UAS technology at each fixed location, and for *ad hoc* or mobile operations. We must conduct specific, data intensive analyses for each potential use 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 FAA nor our partner agencies want to jeopardize safety or interfere with compliant UAS operations.

The FAA is currently working with DOD and DOE to strike that balance as they deploy C-UAS technology at sensitive facilities in the United States. We have forged this new path with DOD and DOE, working through many of the toughest aspects of such deployments in the NAS, such as defining threats, developing concepts of operation, and implementing interagency notification and reporting procedures. We are already sharing these processes and procedures with DHS and DOJ to ensure they benefit from the work we have done with DOD and DOE if they are granted C-UAS authorities and Title 18 relief. We are full partners with DOD and DOE in their efforts to implement this authority, by design of the NDAA, and have received assurances of the same level of commitment to operational collaboration from DHS and DOJ as well.

C-UAS in the Airport Environment

We also note that Congress has expressed interest in granting FAA the authority to test and utilize UAS detection technology. Section 2206 of the 2016 Extension required the FAA, working closely with DHS and other relevant federal agencies, to evaluate detection technology at airports. From February 2016 through December 2017, the FAA and our partner agencies assessed or observed UAS detection technologies operating at several domestic airports in Atlantic City, New York City, Denver, and Dallas-Fort Worth.

The FAA is coordinating its report to Congress on the results of this pilot effort. We learned that the airport environment presents several unique challenges to the use of such technologies. The available technology itself is at an early developmental stage for employment at an airport. The technical readiness of the systems, combined with a multitude of other factors,

such as geography, interference, location of majority of reported UAS sightings, and cost of deployment and operation, demonstrate that this technology is not ready for use in domestic civil airport environments.

In view of these results, the FAA suggests that other actions, such as implementation of remote identification requirements, are more effective and cost-efficient to address the concerns related to non-compliant UAS operations on and around airports. Given the likely resulting impact on the safety and efficiency of manned aircraft operations, compliant unmanned aircraft, and the provision of air traffic services, the FAA does not currently endorse the general use of any mitigation technology on or around an airport. In this case, the use of mitigation technology could introduce more disruption and safety risk than its use is intended to counter.

Enforcement

The interagency work to address the security challenges presented by UAS appropriately has been focused on the risks presented by malicious and 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, not malicious, in nature. These errant operations present a safety concern, which we are addressing in a number of ways. 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 ensure UAS operators understand the rules and responsibilities for flying an aircraft in the NAS.

If an operator is unwilling or unable to comply with applicable regulations, or is deliberately flouting the regulations, we will 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 $1,437 for individual operators to $32,666 for large companies. Congress also gave the FAA authority to assess civil penalties of up to $20,000 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 drone in a way that endangers the safety of the NAS.

To date, the FAA has initiated 74 cases for incidents involving unsafe or unauthorized UAS operations. In 2017, 19 incidents resulted in enforcement actions. In 2016, there were 13 such cases. In addition, 23 cases have been initiated citing the FAA's small UAS rule, part 107. All of those cases involved careless or reckless operations.

The FAA is also engaged in extensive outreach with federal, state, local, and tribal law enforcement entities through its Law Enforcement Assistance Program (LEAP). LEAP activities 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 drone 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 provide them with information regarding the evidence needed by the FAA to take enforcement, as well as to provide a communications link where these law enforcement agencies can pass along reports in a timely manner.

The challenge the FAA continues to encounter in both education and enforcement is the misperception by many recreational UAS operators that they are not required to follow the basic rules of UAS operation because they fit under the statutory exemption for model aircraft

operated under the programming of a community-based organization. These unknowing operators present risks to both manned and unmanned compliant operators. In our view, widely-applicable requirements for remote identification are critical to enabling education and, when necessary, enforcement action when operators conduct non-compliant UAS activity. The current exemption for model aircraft—Section 336 of the FAA Modernization and Reform Act of 2012—makes it difficult for the FAA to develop new regulatory approaches that will help expand and facilitate the greater use of UAS in the NAS. Education, civil enforcement, and a set of basic requirements for all UAS operators are essential to bringing the clueless and careless into compliance; however, our security partners still need the authorities and tools to counter threats from criminals.

Next Steps

As Congress has recognized, remote identification of UAS is a critical step on the path to full integration of UAS technology. In order to ensure that our airspace remains the safest in the world, and to enable our law enforcement and national security partners to identify and respond to security risks, we need to know who is operating in the airspace. Effective integration and threat discrimination will continue to be a challenge until all aircraft in the NAS—manned and unmanned—are able to be identified. Anonymous operations are inconsistent with safe and secure integration.

We recently published the report and recommendations prepared by the summer 2017 UAS Identification and Tracking Aviation Rulemaking Committee (ARC). The ARC's 74 members represented a diverse array of stakeholders, including the aviation community and industry member organizations, law enforcement agencies and public safety organizations, manufacturers, researchers, and standards entities involved with UAS. The ARC's

recommendations cover issues related to existing and emerging technologies, law enforcement and national security, and how to implement remote identification and tracking. Although some recommendations were not unanimous, the group reached general agreement on most issues. The FAA is reviewing the technical data and recommendations in the ARC report to support the development of the FAA's remote ID requirements. We are currently working on a proposed rule to implement these requirements as quickly as possible.

As listed in the Administration's Spring 2018 Unified Agenda of Regulatory and Deregulatory Actions, we have also drafted a security-focused Advance Notice of Proposed Rulemaking (ANPRM) to gain additional information related to the security concerns that impact the advancement of UAS integration. Once issued, the ANPRM will seek information from the public to inform possible rulemaking proposals for reducing risks to public safety and national security as UAS are integrated into the NAS. Consistent with our statutory authority, the FAA seeks to ensure UAS operations will neither create a hazard to users of the NAS or the public at large, nor pose a threat to national security.

On May 9, 2018, the Secretary of Transportation announced that 10 state, local, and tribal governments were selected to participate in the Administration's UAS Integration Pilot Program. Each of the participants will partner with private sector entities to evaluate operational concepts and provide DOT and FAA with actionable information that will accelerate safe UAS integration. The goals of the program are to: identify ways to balance local and national interests; improve communications with local, state, and tribal jurisdictions; address security and privacy risks; accelerate the approval of operations that currently require special authorizations; and collect data to support the regulatory development steps needed to allow more complex, routine low-altitude operations. We are working with each of the participants to identify the

specific operational concepts that the participants will undertake. A list of the participants and each of their proposed operational concepts can be found at: https://www.faa.gov/uas/programs_partnerships/uas_integration_pilot_program/awardees/. We have included, and will continue to engage, our federal security partners in this pilot program.

Conclusion

There is no question that a robust security framework is critical to advancing the Administration's goal to fully integrate UAS into the NAS. By enabling federal security and law enforcement agencies to detect and mitigate UAS threats and risks posed by errant or malicious UAS operations, 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.