



U.S. Department  
of Transportation  
**Federal Aviation  
Administration**

Office of Airports Safety and Standards

800 Independence Ave., SW  
Washington, DC 20591

July 19, 2018

Dear Airport Sponsor:

This supplements the FAA's October 26, 2016, letter distributed to all airport sponsors, a copy of which is enclosed for your reference. This letter provides additional guidance concerning airport interest in evaluating, demonstrating or otherwise deploying unmanned aircraft systems (UAS) detection and countermeasures technology ("counter-UAS") at airports.

The FAA is working to fully integrate UAS into the National Airspace System (NAS) in a safe and secure manner. We are mindful that while UAS technology offers tremendous benefits to our national economy and society, the potential for misuse of this technology poses unique security challenges, particularly in airport environments. We recognize some airports may be interested in researching, evaluating, or deploying UAS detection or other counter-UAS capabilities on or near airports; however, a number of significant safety implications and practical issues, as well as legal restrictions, exist.

First, Section 2206 of Public Law 114-190, the FAA Extension, Safety, and Security Act of 2016 (July 15, 2016), required the FAA to evaluate detection technology at airports. The FAA completed a Section 2206 pilot program carried out under Cooperative Research and Development Agreements (CRDAs) with UAS detection technology manufacturers. The pilot program focused on evaluating certain technology solutions for detecting UAS on and in the vicinity of airports. The FAA did not evaluate countermeasure capabilities in light of the safety implications, operational impacts, and legal constraints discussed further in this letter. The FAA partnered with the Departments of Homeland Security, Defense, and Justice, as well as other Federal Agencies for evaluating detection and countermeasure capabilities. 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.

Through these efforts, we learned the airport environment presents a number of unique challenges to the use of technologies available for civil use. The low 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 this

technology is not ready for use in domestic civil airport environments. In particular, some of the FAA's significant findings and recommendations include—

- Airport environments had numerous sources of potential interference--more than anticipated. High radio spectrum congestion in these environments made detection more difficult and, in some instances, not possible.
- Certain aircraft operational states (e.g., hovering) and the degree of flight autonomy also limit detection. A high level of manpower is required to operate equipment and discern false positives such as when a detection system may falsely identify another moving object as a UAS.
- UAS detection systems should be developed so they do not adversely impact or interfere with safe airport operations, air traffic control and other air navigation services, or the safe and efficient operation of the NAS. They should also work with existing airport systems, processes, procedures, and technologies without modification of current infrastructure.
- The primary factor in determining the feasibility of installing a permanent system at an airport is the number of sensors needed to achieve the desired airspace coverage. Because the coverage volume depends on the unique characteristics and requirements of each airport and the type of system, the number of sensors will vary. The coverage distance for many types of detection technologies also constrains the efficacy of such systems in identifying the locations of UAS.
- Deploying assets in an environment owned by many entities could also make UAS detection systems a challenging solution to acquire and deploy. Overall, costs are prohibitive where higher levels of redundant coverage are required. An additional and critical component of this finding is that technology rapidly becomes obsolete upon installation as UAS technology is rapidly changing.

In addition to these findings and recommendations relative to detection system capabilities, the FAA does not endorse or advocate for the use of countermeasures in the airport environment given the likely resulting impact on the safety and efficiency of the NAS. Further, successful mitigation (using, for example, electronic countermeasure capabilities) is reliant on accurate detection. Therefore, the use of countermeasure technology and the potential response of the targeted UAS when engaged could introduce greater hazards to the NAS than the UAS-based hazard it is intended to mitigate. The FAA expects other actions, such as implementation of UAS remote identification requirements, to be more effective and cost-efficient to address the concern related to non-compliant UAS operations on and around airports.

Remote identification for UAS would enable our security and law enforcement partners to make a more informed determination about whether a particular UAS presents an immediate security threat at a given location and to locate the operator of the suspect UAS. The FAA has initiated rulemaking and is working to develop the policies necessary to implement remote identification requirements. In addition, the FAA is rolling out the Low Altitude Authorization and

Notification Capability (LAANC). LAANC provides small UAS operators a streamlined, efficient, automated solution to enable authorization for airspace access near airports. By September 2018, the National Beta Test of LAANC will be available at nearly 300 air traffic facilities covering approximately 500 airports.

Second, in addition to the safety implications and operational impacts, there are a number of legal obstacles to testing, evaluating, or using countermeasures against UAS, as we indicated in our letter of October 26, 2016. Technologies used to detect or mitigate UAS could implicate various provisions of federal criminal law in title 18 U.S.C. (including, but not limited to the Pen/Trap Statute, the Wiretap Act, the Aircraft Sabotage Act, the Computer Fraud and Abuse Act, and the prohibition against interference with certain satellite operations) as well as other laws, such as the prohibition on Aircraft Piracy in title 49 U.S.C. These statutes have constrained most federal entities from employing technologies which can detect, track, identify, and, when necessary, mitigate UAS that pose a security risk. In addition, the testing, evaluation, and use of such technologies causing intentional EMI to radio communications are subject to statutory restrictions implemented and enforced by the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). Very few entities have obtained legislative relief (or may be otherwise exempt under certain circumstances) from these laws and regulations. We are working closely with our federal security partners to ensure the federal law enforcement community has the tools and authorities necessary to respond to safety and security threats posed by errant or hostile UAS operations and to ensure such actions are carried out in a manner consistent with safe and efficient operation of the NAS.

The evaluation or deployment of UAS detection or countermeasure systems at airports may cause unintentional electromagnetic interference (EMI) and affect the performance of air navigation services equipment on the ground and/or onboard aircraft equipment, as well as necessitate operational procedures to manage the airspace and spectrum impacts created by use of certain types of technology. Therefore, any entities pursuing such evaluations or deployments should coordinate with the FAA to assess and mitigate any potential impacts the technology may have on the NAS. This involves an in depth site- and technology-specific risk-based assessment by the FAA. For use in an airport environment, the necessary FAA coordination would include, at a minimum, coordination with several offices within the FAA's Air Traffic Organization (ATO) (e.g. Technical Operations, Air Traffic Services, System Operations Security, Spectrum Office, Airspace Policy), and other offices such as the Office of Security and Hazardous Materials Safety (ASH) and the Office of Airports (ARP). In addition, the use of certain technologies might, to the extent they involve transmission of radio signals (e.g. radar signals used for detection), require FCC or NTIA authorization and interagency coordination, while certain types of countermeasure technologies may be prohibited based on their capability to cause interference to other authorized radio communications.

Finally, as noted in our October 26, 2016, correspondence, it is important for federally obligated airports to understand the FAA has not authorized any UAS detection assessments at any airports other than those, which previously participated in the FAA's UAS detection program through a CRDA. That work is now complete, and those systems are no longer at the airports. Further, the FAA is not empowered to authorize the assessment or deployment of certain detection capabilities or any countermeasure capabilities at airports. Federally obligated airports

independently allowing evaluations of UAS detection and countermeasure systems could be in conflict with their grant assurances. Without proper advance FAA coordination to identify and mitigate any potential hazards introduced by the system in the airport environment, the use of such systems could place the safety and efficiency of the NAS at risk, which would not be consistent with the airport sponsor's federal grant obligations.

The FAA is committed to working with our federal security partners to ensure UAS are integrated into the NAS in a safe, efficient, and secure manner – which includes enabling an efficient and effective law enforcement response to verified threats in the airport environment. We note that, in the event of a specific threat to safe operations at a particular airport, airport authorities should use their current protocols for alerting the FAA to such concerns; as with all threats to which the FAA is alerted, the FAA will work with our federal, state, and/or local security partners to facilitate an appropriate response.

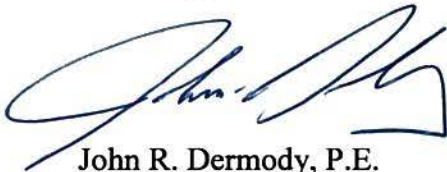
For additional information concerning past UAS detection and countermeasures technology demonstrations, evaluations or deployment at airports, please contact Jim Patterson at 609-485-4989.

Further information on the FAA's UAS integration efforts can be found at:  
<https://www.faa.gov/uas/>

If you have any questions, please feel free to contact me at 202-267-3053.

Thank You.

Sincerely,

A handwritten signature in black ink, appearing to read "John R. Dermody". The signature is fluid and cursive, with a large initial "J" and "D".

John R. Dermody, P.E.  
Director of Airport Safety  
and Standards

Enclosure



U.S. Department  
of Transportation  
**Federal Aviation  
Administration**

Office of Airports Safety and Standards

800 Independence Ave., SW  
Washington, DC 20591

October 26, 2016

Dear Airport Sponsor:

This letter provides guidance on Unmanned Aircraft Systems (UAS) Detection and Countermeasures Technology Demonstrations / Evaluations at airports.

**Background:** The United States Congress charged the Federal Aviation Administration (FAA), under Section 2206 of Public Law 114-190 (July 15, 2016), to “establish a pilot program for airspace hazard mitigation at airports and other critical infrastructure using unmanned aircraft detection systems” in cooperation with the Department of Defense (DOD), Department of Homeland Security (DHS) and other federal agencies. After completion of the pilot program, the FAA “may use unmanned aircraft detection systems to detect and mitigate the unauthorized operation of an unmanned aircraft that poses a risk to aviation safety.” In addition, recognizing the FAA’s long-standing authority, Section 2206 requires consultation with the heads of other agencies to “ensure that technologies that are developed, tested, or deployed by [other agencies] to mitigate threats posed by errant or hostile unmanned aircraft system operations do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.”

The FAA UAS Integration Office is working through Cooperative Research and Development Agreements (CRDAs) with UAS detection manufacturers to evaluate the small UAS detection and identification capabilities, using different methodologies and systems on and near airports. The FAA is also partnering with DHS, DOD and other federal agencies interested in this research, as outlined in Section 2206. These activities have taken place at selected airports around the country, and the agencies are planning additional evaluations later this year and next year.

**Issue:** Recently, technology vendors contacted several U.S. airports, proposing to conduct demonstrations and evaluations of their UAS detection and counter measure systems at those airports. In some cases, the airport sponsors did not coordinate these assessments and demonstrations with the FAA in advance. It is important that federally obligated airports understand that the FAA has not authorized any UAS detection or counter measure assessments at any airports other than those participating in the FAA’s UAS detection program through a CRDA, and airports allowing such evaluations could be in violation of their grant assurances.

Unauthorized UAS detection and counter measure deployments can create a host of problems, such as electromagnetic and Radio Frequency (RF) interference affecting safety of flight and air traffic management issues. Additionally, current law may impose barriers to the evaluation and deployment of certain unmanned aircraft detection and mitigation technical capabilities by most federal agencies, as well as state and local entities and private individuals. There are a number of federal laws to consider, including those that prohibit destruction or endangerment of aircraft and others that restrict or prohibit electronic surveillance, including the collection, recording or decoding of signaling information and the interception of electronic communications content.

Any federally obligated airport that is contacted by a vendor requesting to demonstrate evaluate and deploy any UAS detection or counter measure technology on or near the airport should first contact their local FAA Airport District Office (ADO) before entering into any agreement to conduct UAS detection or counter measure evaluations or demonstrations at their airport. The ADO will then work with the FAA Office of Airport Safety and Standards and the FAA UAS Integration Office to provide a timely response to the airport.

Further information on the FAA's UAS detection efforts can be found at:  
[https://www.faa.gov/uas/programs\\_partnerships/uas\\_detection\\_initiative/](https://www.faa.gov/uas/programs_partnerships/uas_detection_initiative/)

Sincerely,

A handwritten signature in black ink, appearing to read "Michael J. O'Donnell". The signature is stylized and cursive, with a large loop at the end.

Michael J. O'Donnell, A.A.E.  
Director of Airport Safety  
and Standards