ATTACHMENT 2 – FREQUENTLY ASKED QUESTIONS AND ANSWERS CONCERNING UAS DETECTION SYSTEMS

1. What can airports do right now to prepare?

Airport authorities have access to resources, including support from local partners, that may be leveraged to share information on, and to plan and coordinate responses to, potential disruptions caused by errant or malicious UAS operations. Carefully working together, the airport authorities and the FAA, as well as other key stakeholders such as TSA and local law enforcement, can better ensure that airport-specific plans (including any introduction of new technologies such as UAS detection systems) are built around a risk-based, balanced approach that minimizes the potential for the undue impacts on the Nation's aviation system—which none of us want—including disruptions to local air traffic operations and ripple effects that could extend nationally or even beyond. Consistency of response between airports will also be important to air carrier operations.

Some airport authorities have already started to develop plans and capabilities, leveraging immediately available tools and new technologies being advertised by various vendors, to address the unique risks presented by hazardous drone activity. Working with airport authorities will help the FAA to ensure to that these authorities' current and future efforts, including those already underway, are effectively supported and well aligned with our shared goal of sustaining the safety and efficiency of the National Airspace System (NAS). The FAA is currently compiling a checklist of planning factors to consider and key contacts at its national headquarters, with which airport authorities can work in support of our common goal of safety in the NAS.

It is prudent to involve all relevant airport stakeholders in this planning effort, including the FAA (at this early point in these efforts, airport authorities can work with the FAA at the national headquarters level, better enabling the agency to integrate local Air Traffic Control (ATC) input), air carriers and other operators, TSA, and state/local law enforcement with jurisdiction at and around your airport.

2. If a UAS incident happened today, who is responsible for responding?

Consistent criteria, which will be shared among the airport authorities, operators, and various agencies (including the FAA), are still being formulated for determining what constitutes a "UAS incident" that warrants some form of overt

response. Nevertheless, as we recently saw at Newark Liberty International Airport and Dallas/Fort Worth International Airport, as well as in the United Kingdom, drone operations that are perceived to be at least hazardous (if not malicious) are already being encountered and key aviation stakeholders are already taking action.

Currently, drone operations that are perceived to be hazardous can provoke a response from multiple stakeholders: pilots may take tactical action to avoid in-flight encounters; ATC may decide to reconfigure terminal operations, reroute traffic, or even temporarily suspend traffic; airport authorities may opt to alter air field operations, including temporarily closing select runways; and local law enforcement, often at the request of airport authorities or ATC, may dispatch assets on the ground to look for and stop a drone operator.

While hazardous and malicious drone activity poses a number of unique, novel challenges, which are driving the FAA's efforts to work with airport authorities and other stakeholders to establish focused response plans, the various responses being taken today are already built on well-practiced procedures used by these key actors to respond to other safety and security incidents in the NAS, for example when a person aims a laser at an aircraft. These responses are also often coordinated through pre-existing mechanisms such as communication via airport operations centers, direct links to local ATC, and interagency coordination via the Domestic Events Network (DEN). These existing procedures and protocols remain in place for use to the maximum extent appropriate.

Credible reporting and risk assessment are critical prerequisites to any appropriate response. UAS sighting reports may come from a variety of sources, including pilots, airport operators, detection system operators, ATC, airport law enforcement, and even private citizens. The FAA is working with its interagency partners, as well as other key stakeholders in the aviation community, to build mechanisms for assessing the credibility of each report, quickly characterizing risk, and distributing this information through an effective command, control, and communications structure across NAS stakeholders.

In the meantime, maximizing coordination with FAA and other key stakeholders can help airport authorities avoid unilateral, unsynchronized responses that could result in safety and efficiency impacts that outweigh the hazard or threat posed by a given drone incident. A collaborative approach promotes responsible and effective decisions for how to respond to errant or malicious UAS operations.

3) What happens if local resources cannot resolve the issue?

When the full weight of local resources are unable to resolve a credible risk from errant or malicious UAS operations, assistance from federal authorities and supporting resources may be available upon request. There are ongoing discussions within the federal government on how to establish criteria, procedures, and mechanisms for enabling requests for federal assistance. In the meantime, the FAA affirms its commitment to work rapidly with any airport that identifies a credible risk from a UAS.

4) What happens once a request for assistance is made?

The details of the process for responding to a request for federal assistance are still under discussion. Again, we hope to commence discussions with airport authorities in the near future and remain committed to work rapidly with any airport that identifies a credible risk from a UAS.

5) How effective are Counter-UAS systems?

C-UAS has become short hand for both UAS detection and mitigation systems; technically, however, C-UAS only refers to those systems that are used to disrupt, disable, take control of, or destroy a UAS. It is important to discuss detection and mitigation as separate capabilities given the technical and operational considerations associated with each.

The FAA has done an initial evaluation of UAS detection technologies in the airport environment and identified some gaps and challenges as described in our July 19, 2018 letter to airport operators. In addition to concerns regarding the technical performance of UAS detection systems, especially in the complex environment of an airport, airport authorities may wish to carefully consider and work with the FAA to address potentially significant operational pitfalls posed by deploying UAS detection systems, including: determining credibility of detection alerts (e.g., was the detection backed up by visual identification?); differentiating legitimate drone operations from non-compliant activity (e.g., was a detected drone already authorized by the FAA?); characterizing risk (e.g., would a small drone flown by a hobbyist in a remote part of the airport grounds warrant disrupting traffic operations?). The FAA has identified a potential risk to safe airport operations when operational personnel at an airport act upon UAS sighting reports without a comprehensive response strategy that includes coordinated procedures and protocols. Understanding the credibility of reports, including reports of

detection from untested or uncertified systems, is critical to making decisions about appropriate operational response.

With regard to systems that actively interdict offending drones (in other words, C-UAS systems), it should be underscored that only a select few federal agencies (DOD, DOE, DOJ, and DHS) have been granted legal authority by Congress to test and operationally employ active C-UAS systems. This authority was also only granted with strict requirements for use in protection of specific missions, facilities, and assets and only after close coordination with the FAA, which reflects the potential for these systems to cause unintended, significant impacts on the safety and efficiency of the NAS.

In addition, the difficulty in effective response to the persistent disruption of operations at Gatwick, despite the presence of C-UAS systems, underscores the challenges we currently face. The FAA will conduct more detailed C-UAS technology research with our federal agency partners, to include in the airport environment, pursuant to Section 383 of the FAA Reauthorization Act of 2018.

6) Who has authority to deploy and use C-UAS equipment?

The FAA is unable to support the use of counter measure/mitigation systems by anyone but those with explicit statutory authorization; however, coordination with respect to installation and deployment of any detection and mitigation systems put in place by or around an airport assists the FAA in executing its statutorily-mandated duties.

Congress granted Counter-UAS authorities to the Departments of Defense and Energy in December 2016. Recently, in the FAA Reauthorization Act of 2018, Congress granted similar Counter-UAS authorities to the Departments of Homeland Security and Justice. These grants of C-UAS authority are narrowly tailored for use in protection of specific missions, facilities, and assets and only after close coordination with the FAA, which reflects the potential for these systems to cause unintended, significant impacts on the safety and efficiency of the NAS. FAA is working closely with all four departments to support the implementation of those authorities and the deployment of C-UAS systems. At this time, these grants of C-UAS authority are narrowly-tailored for protection of specific missions, facilities, and assets and do not provide authority to deploy and use C-UAS as a standing asset to protect airports. However, DHS and DOJ are assessing how their authorities would cover response to a persistent serious UAS disruption of operations at an airport in the United States.

7) What else is being done?

There are many related efforts that are underway that will make it easier to identify drone operators. The potentially unsafe, unauthorized, and/or malicious use of drones is exactly why the FAA is focused on moving expeditiously with remote identification requirements for UAS in the National Airspace System.

8) What else might an airport authority wish to consider with respect to UAS detection systems?

The FAA is assessing the safety and operational impacts of the use of detection systems at airports. Entities seeking to evaluate or deploy UAS detection systems may take note that the evaluation or deployment of such systems, even systems that are marketed as passive detection systems, may implicate provisions of law (such as title 18 of the United States Code) on which the FAA cannot authoritatively opine. Therefore, the FAA cannot confirm the legality of any UAS detection system. An entity considering installing a UAS detection system may wish to seek system-specific and site-specific guidance from its legal counsel and/or the appropriate authorities.

Licensing through FCC approval and in coordination with FAA's Spectrum Office are required for each site. A vendor might claim that its radar has national spectrum licensing approval, but such approvals are site-specific. A vendor might claim that its radio frequency detection system is passive; however, the system might, in fact, have embedded emitting capabilities that are deactivated by reversible software programming. Some systems might emit for software upgrades or site installation, but be "passive" when operational. For these reasons, we cannot categorically assume any detection system does not impact the NAS. Our July 19, 2018 letter to airport operators discusses coordination with the FAA. To support coordination, we are working to compile a checklist for airport authorities considering the acquisition or use of UAS detection systems at their airports.

Many detection systems may need to be located at high vantage points, due to their direct line-of-sight requirements, and detector arrays may block critical sight lines. Airports must follow all FAA requirements for building structures on an airport. In short, the onus is on the Airport Authority to be cognizant of its federal obligations and local requirements for deployment, zoning, and/or permit

approvals that could impact airport safety—even if located outside the airport property.

Coordination with the FAA helps to promote the best safety outcome when an airport, a third party vendor, or other government or private sector entity locates detection or mitigation systems in and around an airport. The FAA letter dated May 7, 2019, identifies national headquarters points of contact.