

E-ALERT | Government Contracts

April 8, 2013

FAA PROPOSES DRAFT PRIVACY PROVISION TO INCLUDE IN DOMESTIC UNMANNED AIRCRAFT SYSTEM AGREEMENTS AND INVITES COMMENTS

On February 22, 2013, the Federal Aviation Administration (“FAA”) issued [a notice and request for comments](#) with regards to a draft privacy provision in its Other Transaction Agreement (“OTA”) with unmanned aircraft system (“UAS”) test site operators. The provision is the first public effort by any Federal agency to address privacy issues arising from civilian UAS use in the national airspace in contractor agreements, and suggests that Federal agencies may impose similar conditions in agreements involving domestic UAS use in the future.

Below, we provide a brief background of FAA’s UAS regulation efforts and discuss the draft privacy provision as well as remaining questions. As FAA prepares to implement the first privacy provisions relating to UAS use in the national airspace, stakeholders in industry should remain vigilant as future agreements may include similar provisions.

Written comments to FAA’s draft privacy provision are due by April 23, 2013.

I. BACKGROUND ON DOMESTIC UAS REGULATION

The commercial UAS market is projected to grow to \$12 billion per year by 2018. Currently, FAA prohibits the use of UAS in domestic airspace for commercial purposes, and allows public and private entities to use them in domestic airspace only after undergoing a time consuming case-by-case certification processes.

On February 14, 2012, Congress passed the [Federal Aviation Administration Modernization and Reform Act of 2012](#) (“the Act”). The Act mandated that FAA develop widely applicable regulations (without case-by-case certifications) and lead the effort to integrate UAS into the national airspace system by September 30, 2015.

In addition to this September 30, 2015 integration deadline, FMRA sets several milestones for FAA—including publishing a final rule governing operations of small UAS by August 2013 and publishing a notice of proposed rulemaking on all other civil UAS by August 2014. Another of the key milestones was the establishment of six test ranges by August 2012, at which civilian UAS can be operated and tested without full FAA certifications. Though FAA has yet to select test range operators, when implemented, the test ranges will allow FAA to gather “safety and technical information relevant to the safe and efficient integration of UAS into the [National Airspace System] NAS.” The FAA will select test sites and test site operators after consideration of factors such as geographic and climate diversity, the location of necessary ground infrastructure to support the sites, and research needs. Contractors who are selected for each of the sites will be required to enter into an OTA with the FAA, which will set out the legally binding terms and conditions under which the entity will operate each UAS test site.

II. FAA'S DRAFT PRIVACY PROVISION

FAA's February 22, 2013 notice announced a request for proposals for the UAS test sites, and also put forward a draft privacy provision that it intends to include in OTAs with test site operators. The draft privacy provision appears to be the first public step any Federal agency has taken to address privacy concerns specific to UAS operations in the national airspace. As such, although provisions in OTAs are commonly negotiated by Federal agencies without the requirement for notice-and-comment, the FAA provided an opportunity for public input through written and oral comments.

The draft privacy provision would impose significant obligations upon contractors "to operate in accordance with Federal, state, and other laws regarding the protection of an individual's right to privacy." In particular, the draft OTA includes the following requirements: (1) the site operator must post privacy policies publicly for public comment; (2) FAA may modify the OTA to reflect later changes to privacy laws; and (3) only limited data may be transmitted from the site operator to FAA. FAA's approach provides stakeholders with some insight into the mechanism by which privacy issues may be addressed by Federal agencies—in licenses, agreements, and procurements.

If these compliance requirements are adopted, contractors subject to the provision need to examine their privacy policies before they are subject to public scrutiny, and set up a mechanism to solicit and receive public comments. Contractors must also ensure data handling and privacy procedures are in place such that they comply with all applicable local, state, and Federal laws, and transmit (or perhaps collect and store) only the requested data by FAA. For example, contractors need to be cognizant of the varying types of privacy risks that may be presented by different technologies used by UAS. Infrared or thermal sensors could raise significant privacy concerns because they are capable of penetrating ceilings and capturing images of activities and heat sources inside a building. Similarly, UAS sensors could inadvertently capture private information, [as with Google's Street View cars that led to \\$7 million settlement](#), and such information could also be intercepted by third parties, leading to further loss of private data. Indeed, FAA's draft privacy provision may apply regardless of whether the UAS's mission involves surveillance at all, raising significant issues because many types of sense-and-avoid technologies (including commonly used cameras) used to avoid collisions could inadvertently capture private information.

Other questions remain. For example, it is unclear whether privacy restrictions being applied to agreements with operators of UAS will be extended to Government contractors operating manned aircraft, and whether FAA will heed the advice of civil rights organizations that have pressed for increasing FAA regulation of UAS and tighter privacy controls. Questions also remain regarding whether FAA should address privacy issues at all, or instead, whether privacy issues should be left to states or other federal agencies.

We are well positioned to advise clients on the impact of FAA's proposed privacy provisions. If you have any questions concerning the material discussed in this client alert, please contact any of the undersigned.

Susan B. Cassidy
Saurabh Anand

+1.202.662.5348
+1.202.662.5222

scassidy@cov.com
sanand@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein. Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.

© 2013 Covington & Burling LLP, 1201 Pennsylvania Avenue, NW, Washington, DC 20004-2401. All rights reserved.