Comments of the World Privacy Forum
Re: FAA's Unmanned Aircraft System Test Site Program,
Docket No: FAA–2013– 0061

To: U.S. Department of Transportation, Federal Aviation Administration

Via regulations.gov

Attn: Docket Operations, M–30;
U.S. Department of Transportation (DOT)
1200 New Jersey Avenue SE., Room W12–140
West Building Ground Floor
Washington, DC 20590–0001

April 23, 2013

Re: FAA's Unmanned Aircraft System Test Site Program, Docket No: FAA–2013– 0061

The World Privacy Forum is deeply interested in commercial drones and their implications for privacy. On February 14, 2012, Congress mandated that the FAA, coordinating with the National Aeronautics and Space Administration and the Department of Defense, develop a test site program for the integration of unmanned aircraft systems in to the National Airspace System. The FCC has published its proposed policy for the Unmanned Aircraft Systems test sites in the Federal Register for comment. This policy will be applicable to commercial drones operating in the US.

The World Privacy Forum welcomes the opportunity to comment on the FAA's Unmanned Aircraft System Test Site Program. The notice appeared in the Federal Register on February 22, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-22/pdf/2013-03897.pdf. We have included at the end of these comments a section of the original Federal Register notice as an aid to public understanding of these comments.

The WPF is a non-profit public interest research and consumer education group. We focus our activities on privacy issues, and much of our work focuses on technology issues. You can see our publications and more information at www.worldprivacyforum.org.

We congratulate the FAA for taking these first steps on privacy regarding drones. While we are very concerned about how the use of drones will affect privacy, we also acknowledge that there is much that society in general does not know about the use of drones and their consequences for privacy. In addition to privacy, there are a host of uncertain issues surrounding the technology,

the economics, and the law surrounding drones. All of these issues intersect in ways that are unpredictable and as of yet untested and largely unknown.

We offer our comments with that express acknowledgement that everyone has much to learn in this area. The FAA appears to be making good use of the opportunity to advance the learning process for everyone through its Unmanned Aircraft System (hereafter UAS) process. Many of our suggestions below seek to increase general knowledge about drones and their effect on privacy.

1. Clarify applicability of the Privacy Act to UAS test site operators

The FAA should clarify the applicability of the Privacy Act of 1974 to its agreement with the UAS test site operator. Applicability of the Act may depend on any requirements that the FAA might impose on the operator with respect to the collection and maintenance by drones and by the Site Operator of personal information about individuals. We are not necessarily suggesting that the Act must apply because much depends on facts that are not available at present.

2. Determine if Site Operator's activities constitute government action

In a similar vein, the FAA should consider **whether the activities of the Site Operator constitute government action.** The U.S. Constitution limits the ability of the FAA as a government agency to collect some information and to engage in surveillance and other activities. These limits may not apply to the Site Operator. It may be appropriate for the FAA's agreement with the Site Operator to limit Operator activities to those that would be lawful for the government to undertake. The basic policy is that the agreement should not allow the FAA to do indirectly what it is prohibited from doing directly. Frankly, we are not sure that is will be a primary concern at this stage, but as a matter of precedent, we would like to see the government staying clearly within its constitutional and statutory boundaries on privacy matters, whether it acts directly or though an agreement with a private entity.

3. Support for FIPs

We applaud the FAA's citation of Fair Information Practice Principles (FIPs) for core privacy policies, and we support this use. We would prefer that general compliance with FIPs be mandatory, although we would leave some flexibility in the application of the principles because the principles must be adapted to different circumstances. For an introduction to FIPS, see http://www.worldprivacyforum.org/fairinformationpractices.html. For a short history of FIPs, see http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

4. Establish a Privacy Advisory Committee

We also applaud and support the notice requirement that the Site Operator must have a mechanism to receive and consider comments on its privacy policies. With an eye on seeking broad responses to the many privacy issues raised by drones, we suggest that the FAA establish an advisory committee on drone privacy or require the Site Operator to establish a privacy advisory committee. The advisory committee needs to include privacy experts and advocates,

law enforcement, policymakers, and industry. An advisory committee is not the only mechanism for receiving outside comments, but it may be the best way to "contribute to the dialogue among privacy advocates, law enforcement, policymakers, and industry about how to address broader questions relative to the technologies used." The quoted language comes from the abstract to the Unmanned Aircraft Systems Test Site Selection document at https://faaco.faa.gov/index.cfm/announcement/view/13143.

5. Require Site Operators to establish a Chief Privacy Officer

The FAA should require the Site Operator to establish a Chief Privacy Officer (CPO). We are not prepared to state that the function of CPO requires a full-time, dedicated employee. It may be a part time job. However, centralizing the privacy responsibilities in one individual should maximize consideration and coordination of all privacy matters.

6. Mandatory Privacy Impact Assessments

The FAA should require the Site Operator to conduct a full Privacy Impact Assessment (PIA). A PIA should be initiated at the earliest possible time. It would be advisable for the PIA to be an ongoing process rather than a one-time event because understanding of privacy issues will advance over time as technology and operations improve. The PIA might be conducted under the direction of the advisory committee recommended above. We do not propose a specific methodology for the PIA, except to observe that it should not be limited to the PIA required of federal agencies under the Section 208 of the E-Government Act of 2002.

This activity requires a much more robust PIA than the law mandates for federal agencies. The PIA should be published in draft, and the public should have an opportunity to comment. The Site Operator should be required to respond publicly to the PIA and to make changes recommended by the PIA or to explain why the recommended changes were not made. This is the only way to ensure that the PIA will be actually reviewed and not just sit on a shelf.

7. Requirement to publish a FIPs-compliant privacy notice

The Site Operator should be required to publish a privacy notice (as required by FIPs) that, among other things, describes the following:

> a) Plans and policies for the collection, maintenance, use, disclosure, and retention of any potentially identifiable data, including a description of all types of personal data that may be collected, maintained, used, or disclosed. For example, if appropriate, the data types should include images of an individual, a house, a motor vehicle (with or without license plate), and other types of potentially identifiable data.
>
> b) All technologies employed by drones to collect information, including but not limited to photographs, videos, thermal images, automatic license plate readers, facial recognition cameras, and other biometric identification methods).

c) Schedules for record destruction or de-identification of all personal information.

d) Any methods of de-identification used or planned to be used.

e) The procedures that will be used to respond to law enforcement subpoenas, written demands, administrative requests, and the like that seek personal information or potentially identifiable personal information.

f) The procedures that will be used to respond to civil demands for personal information, including whether the Site Operator will provide notice of the demands to the subject of the record demanded.

In closing, we again commend the FAA for giving attention to the privacy issues raised by drones. We observe that the issue of privacy in public spaces is now being generally reassessed as a result of new technology like drones, the Supreme Court's decision in *United States v. Jones* (http://www.law.cornell.edu/supremecourt/text/10-1259), and public surveillance that has become pervasive. The FAA's actions will contribute usefully to that reassessment.

The World Privacy Forum welcomes your questions, and we will be happy to discuss these privacy issues further.

Sincerely,

Pam Dixon
Executive Director
World Privacy Forum
www.worldprivacyforum.org
3108 Fifth Avenue
Suite B,
San Diego, CA 92103
Ph.: 760-712-4281

Addendum

The following information is copied from the Federal Register notice in response to which we have filed these comments. This information in the notice was highly relevant to WPF's comments and may assist the public in understanding our comments.

OTA= OTHER TRANSACTION AGREEMENT
UAS= unmanned aircraft systems

The proposed privacy requirements set forth in Article three of the DRAFT OTA are as follows:

(1) The Site Operator must ensure that there are privacy policies governing all activities conducted under the OTA, including the operation and relevant activities of the UASs authorized by the Site Operator. Such privacy policies must be available publically, and the Site Operator must have a mechanism to receive and consider comments on its privacy policies. In addition, these policies should be informed by Fair Information Practice Principles. The privacy policies should be updated as necessary to remain operationally current and effective. The Site Operator must ensure the requirements of this paragraph are applied to all operations conducted under the OTA.

(2) The Site Operator and its team members are required to operate in accordance with Federal, state, and other laws regarding the protection of an individual's right to privacy. Should criminal or civil charges be filed by the U.S. Department of Justice or a state's law enforcement authority over a potential violation of such laws, the FAA may take appropriate action, including suspending or modifying the relevant operational authority (e.g., Certificate of Operation, or OTA), until the proceedings are completed. If the proceedings demonstrate the operation was in violation of the law, the FAA may terminate the relevant operational authority.

(3) If over the lifetime of this Agreement, any legislation or regulation, which may have an impact on UAS or to the privacy interests of entities affected by any operation of any UAS operating at the Test Site, is enacted or otherwise effectuated, such legislation or regulation will be applicable to the OTA and the FAA may update or amend the OTA to reflect these changes.

(4) Transmission of data from the Site Operator to the FAA or its designee must only include those data listed in Appendix B to the OTA. (Appendix B to the OTA is available as part of the SIR at http://faaco.faa.gov.) The FAA anticipates that test site operator privacy practices as discussed in their privacy policies will help inform the dialogue among policymakers, privacy advocates, and the industry regarding broader questions concerning the use of UAS technologies. The privacy requirements proposed here are specifically designed for the operation of the UAS Test Sites. They are not intended to pre-determine the long-term policy and regulatory framework under which commercial UASs would operate. Rather, they aim to assure maximum transparency of privacy policies associated with UAS test site operations in order to engage all stakeholders in discussion about which privacy issues are raised by UAS operations and how law, public policy, and the industry practices should respond to those issues in the long run.