Departmental Unmanned Aircraft Systems (UAS) Privacy Policy[1]

Background

The Federal Government is committed to ensuring that collection, use, retention, or dissemination of information about individuals through the use of any technology, including unmanned aircraft systems (UAS), complies with the Constitution, and Federal law, regulations, and policies. To that end, agencies must, "prior to deployment of new UAS technology and at least every 3 years, examine their existing UAS policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS, to ensure that privacy, civil rights, and civil liberties are protected."[2] In order to ensure that the Department of Transportation's (Department) use of UAS is consistent with its mission and does not erode the civil rights, civil liberties, and privacy rights and expectations of individuals who may be observed through the Department's UAS activities, the Department has established this UAS Privacy Policy (UAS Privacy Policy). The UAS Privacy Policy provides specific guidance with respect to any UAS operations conducted by the Department (including any of its Operating Administrations[3] and the Office of the Secretary) to ensure that the Department is transparent regarding its activities and that Departmental UAS activities do not create undue privacy risks for members of the public.

This UAS Privacy Policy is the result of consideration of Federal legislation and policy, Departmental policy, and industry best practices. The policy's objective is to enable Departmental mission effectiveness, including but not limited to the Federal Aviation Administration's (FAA) critical research to facilitate the safe integration of UAS in the National Airspace System (NAS), while at the same time preventing inappropriate surveillance and collection of data of or about individuals and ensuring that the appropriate privacy risk analysis is conducted prior to the authorization and commencement of any UAS program or activity.

Purpose

This policy establishes the Department's approach to ensuring that any use of UAS in support of Departmental programs balances programmatic requirements with the need to respect personal privacy and protect individual civil rights and civil liberties.

---

[1] DOT Order 1351.18 Departmental Privacy Risk Management Policy, September 30, 2014 establishes the privacy responsibilities and practices of the Department. The UAS Privacy Policy constitutes a specific set of privacy requirements for UAS operations which must be executed in addition to those established in DOT Order 1351.18.

[2] Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015).

[3] The Department's Operating Administrations are the Federal Aviation Administration, Federal Highway Administration, Federal Motor Carrier Safety Administration, Federal Railroad Administration, Federal Transit Administration, Maritime Administration, National Highway Traffic Safety Administration, Pipeline and Hazardous Materials Safety Administration, and the Saint Lawrence Seaway Development Corporation.

Departmental UAS Privacy Policy

Scope

This policy applies to all Department activities that include the operation of UAS.[4] This policy is informed by the Fair Information Practice Principles (FIPPs).[5] The Secretarial Office or Operating Administration using a UAS will be responsible for ensuring policy requirements are applied to all UAS activities, regardless of where they occur.[6]

Policy

In addition to strict compliance with existing laws and regulations, it is imperative that Departmental UAS operations are conducted in a manner that is consistent with a respect for privacy, civil rights, and civil liberties. Compliance with this policy is mandatory.

The Department will take the following actions to achieve the objectives above:

- The Department's Privacy Risk Management Policy and the FIPPs will be applied to all UAS Operations.
    - The Department's Senior Agency Official for Privacy (SAOP),[7] in consultation with the Office of General Counsel, must conduct a risk analysis of any proposed UAS activity and provide approval prior to the commencement of UAS operations. Any mitigation strategies identified in the risk analysis must be implemented prior to UAS operations. [8]
    - All proposed UAS operations will be analyzed by the SAOP to ensure they meet privacy regulations, statutes, and guidance. The privacy analysis will be documented and made available to the public as appropriate. In addition, any significant or material changes to existing UAS operations are required to be reviewed consistent with the Department's Privacy Risk Management Policy. Examples of significant or material changes in operations include but are not limited to introduction of new data collection techniques (e.g., radar to camera) and changes in operating areas (e.g., rural to urban).
    - The Department will include appropriate privacy requirements, including requiring compliance with this UAS Privacy Policy, in all DOT contracts involving the use of UAS.

[4] This policy does not cover the Office of Inspector General (OIG). Should the OIG conduct UAS operations, the OIG, in consultation with the Senior Agency Official for Privacy, will publish a privacy policy for its UAS operations.

[5] Transparency, Individual Participation, Purpose Specifications, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

[6] Secretarial Offices or Operating Administrations conducting UAS activities on behalf of other government or private sector entities are responsible for notifying the Senior Agency Official for Privacy of such activity.

[7] Per the Department's Privacy Risk Management Policy, the SAOP may direct the Departmental Chief Privacy Officer to conduct and document any necessary analysis and provide recommendations.

[8] As appropriate, the documented risk analysis will be conducted using the DOT Privacy Office established Privacy Threshold Assessment (PTA) and include an assessment of risk and mitigations of any impacts to individual civil rights or civil liberties resulting from the proposed UAS operations.

- To the extent practicable the Department will ensure that UAS operations do not intentionally collect personally identifiable information (PII)[9] which includes imagery, phone, wireless, and any other electronic emissions that might contain PII, unless authorized by law and necessary to accomplish Departmental mission.
    - In the event that PII is collected unintentionally, the Department office using the UAS will notify the SAOP and obscure or remove identifying data to the extent practicable immediately upon discovery of the PII, but no later than 180 days after the collection unless retention is necessary to fulfill an authorized mission of the Department or is required to be retained for a longer period in order to comply with existing law or regulation.
- Ensure all individuals involved in the operations of UAS are appropriately trained and supervised to ensure compliance with this policy and any specific privacy risk mitigation strategies established by the SAOP for approved UAS operations.
- Provide advanced public notice of planned flight operations through local media or a publicly posted web site.

Compliance & Audit

The Department's SAOP shall conduct an annual privacy review of the Department's use of UAS to ensure compliance with existing law, regulations, and Department policy, and to identify potential privacy risks. Where appropriate, the SAOP will make recommendations to ensure that the Department's use of UAS is consistent with its authorities and applicable law, regulations, and policies. The outcomes of this annual review will be made publicly available in a forum that provides an opportunity for public feedback.

This policy will remain in effect until superseded by an authorized update.

RICHARD MCKINNEY

Digitally signed by RICHARD MCKINNEY
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=RICHARD MCKINNEY
Date: 2016.06.03 14:18:07 -04'00'

[9] "Personally identifiable information" refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, as set forth in Office of Management and Budget memorandum M-07-16 (May 22, 2007) and Office of Management and Budget memorandum M-10-23 (June 25, 2010).