U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Unmanned Aircraft Systems (UAS) Support Center Case Management System (CMS)

Responsible Official

1.0 Danielle Corbett
2.0 Email: Danielle.Corbett@faa.gov
3.0 Phone Number: 404-579-8613

Reviewing Official

4.0 Karyn Gorman
Acting, Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

[Publication Date]

Executive Summary

The Federal Aviation Administration (FAA) developed the Unmanned Aircraft Systems (UAS) Support Center Case Management System (CMS) which is a system allowing members of the public (hereafter referred to as customers) to submit inquires about their UAS and for the FAA to track and respond to those inquires. Inquiries submitted by customers could include general questions as well as the operation of a UAS.

The FAA is publishing a Privacy Impact Assessment (PIA) in accordance with Section 208 of the E-Government Act of 2002 because the UAS Support Center CMS collects the name, preferred method of communication, email address or phone number, and optional zip code from the customer when submitting an inquiry about their UAS.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Federal Aviation Act of 1958 gives the FAA the responsibility to carry out safety programs to ensure the safest, most efficient aerospace system in the world. The FAA is responsible for:

- Regulating civil aviation to promote safety;
- Encouraging and developing civil aeronautics, including new aviation technology;
- Developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- Developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- Regulating U.S. commercial space transportation.

The FAA UAS Support Center was first established in December 2015 to help implement the first-ever FAA regulation for UAS – the Part 48 Registration and Marking Requirements for Small Unmanned Aircraft. At the time, the public had a lot of questions and concerns about this new rule and the Support Center operated around the clock to answer questions, listen to concerns, and try to normalize the FAA's role in the UAS industry. For many people, this was their first introduction to the FAA.

As the registration rule was rolling out, the FAA was also working on the first operational rule for UAS known now as Part 107-Small Unmanned Aircraft Systems. Given the rapid growth of the UAS industry and the pace of new statutory and regulatory requirements, the FAA quickly realized that the Support Center would continue well beyond these early days of change.

Today, the Support Center serves as the front door for people who are new to flying UAS, are looking for guidance on how to operate safely in various environments, or have questions about the role UAS play in the broader aviation community. The FAA developed the Unmanned Aircraft Systems (UAS) Support Center CMS to track and respond to customer inquiries that were previously submitted by email.

The UAS Support Center CMS is a public, web-based application for the customers to submit inquiries about their UAS and for the FAA to track and respond to the inquires. Customers are not required to login or authenticate to the system to submit an inquiry. The form will be accessible as a link on the FAA UAS Contact Us page: https://www.faa.gov/uas/contact_us where customers can submit their inquiries by completing a Customer Inquiry form that collects the name, preferred method of contact, email address or phone number, and have the option to provide their zip code. The customer selects the demographic category for which they can be identified (i.e. recreational flyer, business flyer, public safety, local government,

educational/research, I Don't Know or other) from a drop down box. Finally the customer enters the subject and in an open comment box, details about the inquiry they are submitting.[2]

The customer submits the inquires ranging from the customer's operation of an UAS to general UAS questions. Once submitted, the UAS Support Center CMS generates a reference number used to track the inquiry and sends the customer an automated email including the reference number, creation date, demographic subject, and inquiry description. For customers who have opted to use their phone as the preferred method of contact, an analyst would call and provide the forementioned information.

Customers can check the status of their inquiry at link on the FAA UAS Contact Us page: https://www.faa.gov/uas/contact_us by entering their reference number and email address. Once the system confirms the reference number and email address match with the inquiry record in the system it will display the inquiry status as new, in progress, escalated, reopened, or closed and creation date of the inquiry. No personally identifiable information (PII) is viewable to customers when checking the status of their inquiry.

The UAS Support Center analyst logs into the system using their Personal Identity Verification (PIV) card and selects an inquiry record to work. The inquiry record displays the customer's name, email address or phone number. The analyst communicates with the customer by the selected preferred method (email or telephone call). The analyst enters the information the communication into UAS Support Center CMS and that information is only viewable to the Support Center.

Once the inquiry is resolved, the Support Center analyst will close the inquiry and either the system sends an email or a support center analysts calls the customer to notify them the inquiry has been resolved and closed. The email contains a link to a customer feedback survey that remains active for 30 days for customers to provide feedback at their discretion (customers will not receive a survey link over the phone). The survey will include the following questions:

- Rating of overall satisfaction – 5 star rating
- Any comments about overall satisfaction – short text box
- Resources used to contact UAS support center – check all that apply picklist (Web Search, Vendor, DroneZone, None, and Other)
- Rate your overall satisfaction (Other than the Support Center) – 5 star rating
- Any comments about overall satisfaction - short text box
- How FAA can make it easier for members of the public to understand information about drone safety and regulations - long text box
    - Receive occasional emails from the FAA UAS Support Center CMS about drone safety – yes or no checkbox.

UAS Support Center CMS collects and maintains the survey replies from the customer and links these survey replies to the specific case. Only the UAS Support Center CMS administrator will have access to the name of the respondents once responses are received.

[2] The open comments box in the system includes a message to customers not to submit Personally Identifiable Information (PII) with their comments.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) v3[3], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[4].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

UAS Support Center CMS collects the name, email address or phone number, and (optionally) zip code directly from the customer. A reference number is generated to track the customer's inquiry. The inquiry is retrieved by reference number or email address however, the record that is returned is not about the customer but about the inquiry status. According UAS Support Service CMS is not a Privacy Act System of Record.

The publication of the PIA demonstrates DOT's commitment to provide appropriate transparency to UAS Support Center CMS.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

The UAS Support Center CMS collects the name, email address or phone number, and (optionally) the zip code directly from the customer. Records maintain in UAS Support Center

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[4] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

CMS are not subject to the Privacy Act. The customer can access the system and check the status of their inquiry but are not able to amend. If the record requires amending, they can contact the UAS Support Center and they can amend the record.

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

The Federal Aviation Act of 1958 is the legal authority that authorizes the FAA to collect information from customers submitting an inquiry. UAS Support Center CMS collects the name, email address, phone number and zip code as an option from the customer when submitting their inquiry about their UAS. The name and email address is used to communicate with the customer. The email address will also be used to send out a survey in which is the customer has the option to complete. The zip code option but if provided will allow the analyst to more efficiently address the inquiry. For example the analyst can use the zip code to identify trends in a specific area and identify if flying is permitted in that airspace. UAS Support Center CMS also generates a reference number that is used to track the status of the inquiry.

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

The UAS Support Center CMS collects the minimum amount of PII necessary to process the customer's inquiry. Records are maintained in accordance with the National Archives and Record Administration (NARA), General Records Schedule (GRS) 6.5, Public Customer Service Records and records are destroyed 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The UAS Support Center CMS does not share information with external systems.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s). TRANSereve's WebApplicaiton has it's own interal process for ensuring that the correct types of info are inputted such as only letters included in name fields and not numbers etc.

The customer is responsible for ensuring the accuracy of the information they enter when submitting an inquiry. The Customer Inquiry form has data input validation measures requiring data input follows expected formats for phone numbers (following typical US Domestic and International formats) and email addresses.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

The UAS Support CMS protects PII against loss, unauthorized access, or compromise with reasonable administrative, technical, and physical security safeguards. Authorized FAA users access the system using their PIV card.

Training is required for FAA users depending upon their roles and responsibilities. All FAA employees and contractor personnel must complete privacy and security training and agree to the Rules of Behavior (ROBs), which emphasize privacy protective practices. The UAS Support Center CMS received its Authority to Operate (ATO) on 23 November 2021.

FAA incorporates standards and practices required for federal information systems under the Federal Information Security Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, dated March 2006, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, dated September 2020.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

The FAA's Office of the Chief Information Officer, Office of Information Systems Security, Privacy Division, is responsible for governance and administration of FAA Order 1370-121B,

FAA Information Security and Privacy Program and Policy. FAA Order 1370-121B implements the various privacy laws based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-3470, the Federal Information Security Management Act (FISMA), Department of Transportation (DOT) privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

In addition to these practices, additional policies and procedures have be consistently applied, especially as they relate to the protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The users of the UAS Support Center CMS have been informed and trained on the appropriate procedures to notify the necessary DOT and FAA representatives in case of a data spill or breach. The DOT Privacy Office and the FAA Security Compliance Division (AIS-200) will conduct periodic privacy compliance reviews of UAS Support Center CMS with the requirements of OMB Circular A-130.

Responsible Official

Danielle Corbett
System Owner
Manager, Operational Program Branch, Aviation Safety

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Acting, Chief Privacy & Information Asset Officer
Office of the Chief Information Officer