U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)

Declaration of Compliance (DECMAN)

Responsible Official

Gary R. Loving
Enterprise Program Management Services, UAS Program Office Division, AEM-210
gary.r.loving@faa.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

CLAIRE W BARRETT Digitally signed by CLAIRE W BARRETT
Date: 2021.03.15 13:10:04 -04'00'

Executive Summary

The Federal Aviation Administration's Declaration of Compliance (DECMAN) system is used by applicants to submit declaration of compliance (DOC) with the design and production rules for small Unmanned Aircraft Systems (UAS) and demonstrate their means of compliance for approval by the FAA. The DECMAN system supports processing of applications for DOCs submitted under both the Operation of Small Unmanned Aircraft Systems Over People and Remote Identification of Unmanned Aircraft Systems rulemakings. The FAA is developing this Privacy Impact Assessment in accordance with Section 208 of the E-Government Act of 2002 because the system collects personally identifiable information of members of the public including: applicant's name, mailing address, phone number, email address, and company name (optional).

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;*

[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).

- *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.*

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

Operations Over People

In the FAA Modernization and Reform Act of 2012 (Public Law 112-95), Congress mandated that the Department of Transportation (DOT) conduct a suite of rulemakings to integrate small Unmanned Aircraft Systems (UAS) into the National Airspace System (NAS). Based on this direction, the Department of Transportation and the FAA promulgated 14 Code of Federal Regulations (CFR) part 107, which allows operations of small UAS under the Operation and Certification of Small Unmanned Aircraft Systems final rulemaking (June 28, 2016). In 2018, Congress updated the authority basis for part 107, which is now codified at 49 United States Code (U.S.C.) 44807. Part 107 currently prohibits operations of small UAS at night, over people, and over moving vehicles in the absence of a waiver that allows such an operation.

The FAA published the Operation of Small Unmanned Aircraft Systems Over People Notice of Proposed Rulemaking on February 13, 2019, and the final rule on January 15, 2021. The proposed and final rules allow for routine operations of small unmanned aircraft over people under certain conditions. An applicant who seeks to establish eligibility of the small UAS to conduct Category 2 or 3 injury severity thresholds, or both, operations over people will submit a declaration of compliance to the FAA that asserts compliance with the performance-based requirements of the rule. Before a UAS can conduct Category 2 or 3 operations over people, the applicant must demonstrate that the small UAS meets the requirements. An applicant would use an FAA-accepted Means of Compliance (MOC) to show that its small UAS meets the requirements of the rule. An MOC is the term the FAA uses for the method an applicant would use to show that its small unmanned aircraft meets the requirements applicable to Category 2 or 3, or both. The FAA does not tell applicants which method to use to establish compliance; rather, the rule allows the applicant to develop a method and present evidence to the FAA showing that the method is appropriate and accurately demonstrates compliance. The applicant then submits a DOC to the FAA that certifies compliance with the applicable requirements. The majority of applicants that submit DOCs with regard to operations over people are expected to be companies and other business entities; however, there will also be DOCs submitted by applicants who are individual members of the public.

Remote ID

On December 31, 2019, the FAA published a notice of proposed rulemaking titled Remote Identification of Unmanned Aircraft Systems that would require remote identification of unmanned aircraft systems operated in the airspace of the United States that would address safety, national security, and law enforcement concerns regarding the further integration of these aircraft into the airspace of the United States while also enabling greater operational capabilities. The FAA published the final rule on January 15, 2021. One element of the rulemaking includes the FAA's requirement that all persons responsible for the production of standard remote identification unmanned aircraft and remote identification broadcast modules must submit a DOC for acceptance by the FAA. The person responsible for the production of standard remote identification unmanned aircraft or remote identification broadcast modules requesting acceptance of a DOC must declare that the unmanned aircraft or broadcast module complies with the minimum performance requirements of 14 CFR part 89. After the compliance date of the operating requirements of the final rule, any person operating an unmanned aircraft with remote identification in the airspace of the United States will be prohibited from doing so unless the standard remote identification unmanned aircraft's or remote identification broadcast module's serial number is identified on an FAA-accepted DOC, or the UAS without remote identification is operated within the boundaries of an FAA-recognized identification area. Manufacturers submitting DOCs in compliance with remote identification requirements are expected to consist exclusively of companies and other entities, rather than individuals.

Declaration of Compliance

The FAA developed the DECMAN system to process operations over people and remote identification DOCs to meet the requirements of both the small UAS Operation Over People and the Remote ID rulemaking efforts. To register a user account, an applicant navigates to uasdecman.faa.gov and enters their name, address, e-mail address (also their user name), company (optional) and creates their password. Once they receive confirmation of account creation, the applicant then logs into their user account and selects either a declaration for operations over people or remote identification of unmanned aircraft. Both application types use an electronic form[2] to collect the following information from applicants:

- An applicant's name will auto populate with the information provided in the account setup;
- Applicant's contact information (mailing address, phone number, and email address);
- Aircraft description (make, model and series; serial number or range of serial numbers for which compliance is declared);
- For remote identification broadcast modules, the make and model, as well as the serial number, or the range of serial numbers for which compliance is declared;

[2] OMB information collection request numbers 2120-0781 and 2120-0775

- For operations over people, the applicant must provide the (injury severity limit) category to be declared;
- The means of compliance used in the production of the unmanned aircraft or broadcast module;
- The applicant must also identify if the DOC is an initial declaration or an amended declaration, and if amended, the reason for resubmittal; and
- Submit a certification that the applicant has demonstrated that the unmanned aircraft or remote identification broadcast module meets the requirements of the rule through an accepted MOC.

In addition to providing the above mentioned PII and compliance information, the applicant must comply with the following statements in order to receive approval from the FAA:

For small UAS Operations Over People:

- Certification that the small unmanned aircraft satisfies the impact kinetic energy and exposed rotating parts standards of that category through an accepted means of compliance;
- Certification that the manufacturer has a product support and notification process; and
- Certification that the Administrator will be allowed to inspect the manufacturer's facilities, technical data, and any manufactured small unmanned aircraft, and witness any tests necessary to determine compliance.

For remote identification of unmanned aircraft:

- A person responsible for the production of standard remote identification unmanned aircraft or remote identification broadcast modules must demonstrate that the standard remote identification unmanned aircraft or remote identification broadcast module was designed and produced to meet the minimum performance requirements of part 89 by using an FAA-accepted means of compliance.
- A person responsible for the production of standard remote identification unmanned aircraft or remote identification broadcast modules must, upon request, allow the Administrator to inspect the person's facilities, technical data, and any standard remote identification unmanned aircraft or remote identification broadcast modules the person produces, and to witness any tests necessary to determine compliance with part 89 subpart F.
- A person responsible for the production of standard remote identification unmanned aircraft or remote identification broadcast modules must cause independent audits to be performed on a recurring basis, and additionally, whenever the FAA provides notice of noncompliance or potential noncompliance, to demonstrate the standard remote identification unmanned aircraft or remote identification broadcast modules listed under a declaration of compliance meets the requirements of part 89 subpart F. The

person responsible for the production of standard remote identification unmanned aircraft or remote identification broadcast modules must provide the results of all such audits to the FAA upon request.

- A person responsible for the production of standard remote identification unmanned aircraft or remote identification broadcast modules must maintain product support and notification procedures to notify the public and the FAA of any defect or condition that causes the standard remote identification unmanned aircraft or remote identification broadcast module to no longer meet the requirements of part 89 subpart F, within 15 calendar days of the date the person becomes aware of the defect or condition.
- A person responsible for the production of a remote identification broadcast module must make available instructions for installing and operating the remote identification broadcast module to any person operating an unmanned aircraft with the remote identification broadcast module.

Applications without an FAA-accepted MOC are not accepted and applicants are prompted to provide an FAA-accepted MOC to move forward with submitting their application. The applicant will receive an email, stating that their DOC has been rejected or accepted. An application is rejected when the MOC used has been rescinded. The applicant will receive an email that will include information about the rescission and be asked to submit an FAA-accepted MOC for acceptance of their DOC application. Once the applicant provides an FAA-accepted MOC, the application can be accepted for review.

To review the DOC, FAA employees access the system using their Personal Identity Verification card to determine if the means of compliance meets the standards. If the declaration of compliance is accepted, the applicant will receive notification by email address provided that their application is approved.

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

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf

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.

The majority of applicants that submit a DOC are companies and not individuals. In those instances in which applicants are individuals, DECMAN does not retrieve records by a unique identifier linked to an individual rather, records are retrieved using information relating to the aircraft. Records maintained by DECMAN are associated with the aircraft and not an individual. Accordingly, DECMAN is not a Privacy Act system of record.

There are several methods of communication used to inform the public of small UAS related information that the FAA would collect, used or maintain. On Machr 18, 2019, the FAA published a Small UAS Over People Notice of Proposed Rulemaking PIA. In addition, the FAA published PIAs for the Remote Identification of UAS final rule on January 15, 2021 and the Operation of Small UAS Over People Final Rulemaking on January 15, 2021. The proposed notice for the Remote ID of UAS and Operation of Small UAS Over People rulemakings are already published in the Federal Register. The FAA will also communicate with the general public on the DOC requirements through platforms, including FAA websites, the news, and social media.

The publication of this PIA further demonstrates the DOT's commitment to provide appropriate transparency into the DECMAN.

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.

DOC applicants voluntarily provide their name, mailing address, phone number, email address, company name, the make and model of the remote identification broadcast module, and remote identification broadcast module serial number as part of the compliance process. Applicants can correct or amend their information while completing the application. If an

[4] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

applicant determines that information within DECMAN is inaccurate, the epplican can log in and amend all information with the exception of their name and company name, make and model. To amend those tiems the applicant would have to contact the help desk to make appropriate updates to this information.

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.

DOC applicants provide their name, mailing address, phone number, and email address, as this information is used to contact the applicant if there are questions pertaining to the DOCs they have submitted. Additionally, the applicant provides the make and model, as well as the serial number of the remote identification broadcast module as this information is used to process and approve operations over people and remote identification DOC applications. The authorities for the collection of information for both final rulemakings are as follow:

- 14 CFR § 107.155 – Means of Compliance. Any person who seeks FAA acceptance of a means of compliance with the performance-based standards of the final rule will be required to submit information in support of the request for FAA acceptance. Manufacturers may submit means of compliance in conjunction with their Declarations of Compliance, to request contemporaneous FAA acceptance of them.
- 14 CFR § 107.160 – Declaration of Compliance for Manufacturers. Any manufacturer that seeks to qualify a small UAS for operations over people under two of the three categories the FAA proposes to permit must submit a Declaration of Compliance to the FAA in a form and manner acceptable to the FAA Administrator.
- 49 U.S.C. 106(f), 40101 note, 40103(b), 44701(a)(5), 46105(c), 46110.– Authorizing the Administrator to prescribe regulations, standards, and procedures and issue orders with respect to aviation safety.
- 14 CFR § 48.110 – Application for Registration. Establishes the information that must be submitted by each applicant for a Certificate of Aircraft Registration.
- 14 CFR § 89.130 – Confirmation of Identification. Any person who wishes to operate a foreign registered civil unmanned aircraft in the United States must provide, prior to the operation, certain information about the operator and the standard remote identification unmanned aircraft or remote identification broadcast module in a notice of identification.
- 14 CFR § 89.210 – Requests for establishment of an FAA-recognized identification area. A community based organization or educational institution requesting establishment of a flying site as an FAA-recognized identification area would need to provide contact information for a representative for communications with the FAA.

- 14 CFR § 89.405 – Means of Compliance. Any person who seeks FAA acceptance of a means of compliance will be required to submit information in support of the request for FAA acceptance. Applicants may submit means of compliance in conjunction with their declarations of compliance, to request contemporaneous FAA acceptance of them.
- 14 CFR § 89.530 – Submission of a declaration of Compliance for FAA acceptance. Any person responsible for the production of standard remote identification unmanned aircraft or remote identification broadcast module who seeks to declare an unmanned aircraft or broadcast module as remote identification compliant must submit a declaration of compliance to the FAA in a form and manner acceptable to the FAA Administrator.

In the event of an accident, contact information may be shared with law enforcement. There will be no additional sharing of this information with external agencies.

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 FAA collects name and contact information of individuals submitting DOC in order to correspond with them regarding their application. No other additional information about the individual is collected or required.

The FAA is proposing maintaining proposes to maintain the records for two years after business use ceases (manufacturer no longer participates in the operation and certification of small UAS). The retention of the records will allow the processing and approval of DOC applications. DOC will be maintained as permanent records until the records schedule (see job number DA DAA-0237-2021-0004) is approved by NARA.

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 FAA may share the aircraft make/model information with other FAA systems to facilitate aircraft registration. The contact information of the DOC applicant is not shared with other FAA systems.

The FAA will make publically available a list of producers of the unmanned aircraft models and remote identification broadcast modules that are compliant with the MOC. The listing will include the status of each applicant's declaration of compliance for their unmanned aircraft and remote identification broadcast modules by make, model, and series, and if applicable, by serial number and category. This will enable remote pilots to determine which

unmanned aircraft and remote identification broadcast modules meet the requirements of the remote identification and operations over people rules, respectively.

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).

Individuals submitting DOCs to the FAA in electronic form are responsible for ensuring the accuracy of their own data. Information collected during the application process can be amended as needed. Systems that collect information electronically have technical capabilities such as data field checks (e.g., ensuring numeric digits or symbols are not entered into name fields) to support accurate data submissions. The DOC applications include applicant contact information, so the FAA can follow up with them as needed if there are issues or concerns with the applications.

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 FAA protects PII with reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate 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 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

The DECMAN is a low risk system and expected to receive its three-year authority to operate in March 2021. Access to the DECMAN system is limited to those with appropriate security credentials, an authorized purpose, and need-to-know. The FAA deploys role-based access controls in addition to other protection measures reviewed and certified by the FAA's cybersecurity professionals to maintain the confidentiality, integrity, and availability requirements of the system.

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 1370.121, FAA Information Security and Privacy Program Policy. FAA Order 1370.121 implements the various privacy requirements based on the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the FISMA, DOT privacy regulations, Office of Management and Budget (OMB) mandates, and other applicable procedures and guidance.

In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees are given clear guidance regarding 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 FAA periodically conducts privacy compliance reviews of all FAA systems that retain and/or process PII with the requirements of the OMB Circular A-130.

Responsible Official

Gary R. Loving
System Owner
Enterprise Program Management Services, UAS Program Office Division, AEM-210

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer