U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration (FAA)
Office of Aviation Safety (AVS)
National Automated Conformity Inspection Process (NACIP)

Responsible Official

Harish Pai
Email: Harish.Pai@faa.gov
Phone Number: (405) 954-8028

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The Federal Aviation Administration's (FAA) Office of Aviation Safety (AVS) owns and operates the National Automated Conformity Inspection Process (NACIP) system that operates under the authority of 49 U.S.C. § 329(b). NACIP is used by Designated Airworthiness Representatives (DARs), Designated Manufacturing Inspection Representatives (DMIRs), Designated Engineering Representatives (DERs), Organization Designation Authorization (ODA) personnel, or someone working on their behalf (hereafter referred to as "designees"[1]) to create the *FAA Form 8120-10, Request for Conformity (RFC)*. Additionally, NACIP is used to submit the FAA Form 8120-10 to the Certification Branch (CB) and/or Certification Management Office (CMO) to conduct a conformity inspection.

The FAA is publishing this Privacy Impact Assessment (PIA) for NACIP in accordance with Section 208 of the E-Government Act of 2002, because NACIP maintains Personally Identifiable Information (PII) from members of the public, including the designee's name and designee number, or the name of someone operating on behalf of the designee. In addition, NACIP maintains PII from FAA employees and FAA contractors.

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.[2]

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

[1] A designee is a private person or organization designated to act as a representative of the Administrator.
[2]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).

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.*

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 Federal Aviation Administration (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.

When the applicant needs to create a design or change the design type for a certified aircraft-related product, the FAA must approve the change. The applicant for the design change/approval submits a proposed certification matrix plan that identifies which rules they are going to show compliance to the FAA. Furthermore, the applicant identifies design and production documents generated as part of a design for approval. The conformity inspection is a step within the FAA certification process for design approval. The NACIP Request for Conformity (RFC), described further below, is a tool used to verify that the aircraft conforms to an approved design type. Also, it is used to conform certain aspects of the design or conform test plan set-ups, which are not part of the type design.

Designees use NACIP to create the *FAA 8120-10.pdf* to initiate the conformity inspection. The conformity inspection process evaluates the aircraft, its parts, assemblies, and

installations to an approved design. The type certification [3] approves the design of the aircraft and all component parts (including propellers, engines, etc.). The NACIP business processes are described below.

System Access

NACIP is accessible to both internal (FAA employees and contractors) and external (designee) users at https://nacip.faa.gov. Internal users log into NACIP using their Personal Identity Verification (PIV) Card. First-time external users must create a user account. They provide their name and email address and either provide the last four of their social security number (SSN) or a government-issued ID, which FAA's MyAccess system collects and shares with a third party to confirm the user's identity to create a NACIP account. Once an external user account is created, they access NACIP via MyAccess by entering their username and password. For a full discussion of the process, see the MyAccess PIA.

Request for Conformity Inspection (RFC)

When the FAA receives the FAA Form 8110-12, *Application for Type Certificate, Production Certificate, or Supplemental Type Certificate* from the applicant, which includes a drawing for the project, an FAA design approval project is opened by the Office of Aviation Safety (AVS) Certification Branch (CB) into the Certification Project Notification (CPN) system. CB personnel use FAA Form 8110-12 as the source of the company name and address and add the information into CPN to obtain a project number. Once a drawing is approved, the CB initiates a NACIP Project RFC inspection for the drawing. The CB sends a written notification to the applicant identifying the FAA project number for the request. The designee logs into NACIP to create the RFC. There are four types of RFCs: Project RFC, Production RFC, International RFC Routing Sheet, and Type Inspection Authorization (TIA) Routing Sheet. Of the four, only the Project RFC is accessible to internal and external users. The other RFCs are only accessible to internal Certification Management Office (CMO) users.

Upon selecting an RFC, the designee enters the project number, which NACIP shares with CPN for validation. Once validated, CPN populates NACIP with the applicant's name. The remaining fields in the form are filled out by selecting the appropriate information from drop-down boxes. The designee's name is selected from the NACIP designee drop-down list. This information is pulled from the Designee Management System (DMS), which

[3] Type Certification is how the FAA manages risk through safety assurance. It provides the FAA confidence that a proposed product or operation will meet FAA safety expectations to protect the public. Certification affirms that FAA requirements have been met. Further information concerning different certifications used in aircraft manufacturing, can be found at the FAA's website: https://www.faa.gov/uas/advanced_operations/certification.

includes the designee's name, email address, and phone number (the email address is not listed in the NACIP form).

For each request, supporting documents and additional forms may be uploaded to NACIP. The uploaded information could include drawings, test plans, and FAA Forms, such as *FAA Form 8130-3 Authorized Release Certificate, Airworthiness Approval Tag*, *FAA Form 8130-9, Statement of Conformity (Statement of Conformity)*, *FAA Form 8110-3*, *Determination of Compliance with Airworthiness Standards*, *FAA Form 8110-1 (Type Inspection Authorization)*, *8100-1, Conformity Inspection Record (faa.gov)*. Once the *FAA Form 8120-10, Request for Conformity (RFC)* is completed, it is submitted to the CB for the RFC to be logged into NACIP. NACIP generates a tracking number during RFC Login to track the conformity through the RFC process. An email is sent to CMO through NACIP that includes the tracking number. NACIP is not used for the design approval, it is only used to manage the conformities during the design approval project. Once the NACIP conformity is completed, it is reviewed by the CMO, then by the CB, and closed by the CB.

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[4], 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[5].

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.

NACIP does not collect information directly from an individual, but receives information from other FAA systems, such as CPN and DMS. Notice is provided at the

[4] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[5] https://csrc.nist.gov/publications/detail/sp/800-53a/rev-5/final

initial point of collection. Records are retrieved by an identifier such as name, however, the records are not about an individual, but about the aircraft. Therefore, these records are not subject to the Privacy Act. The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency for NACIP.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, 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.

NACIP obtains information from CPN and DMS. It is not the original point of collection for the designee's PII. As such, the information that NACIP receives from CPN and DMS is assumed to be accurate. The information collected in DMS may be covered by the Privacy Act. To pursue redress for information processed through DMS, please reference the DMS PIA

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.

NACIP operates under operating authority 49 U.S.C. § 329(b) and is used by designees to create the FAA Form 8120-10, *Request for Conformity (RFC)*. NACIP maintains the following information to track the RFC:

Full name, FAA email address, FAA telephone number, and FAA role on employees and inspectors who access the system and complete inspections.

(DAR or DMIR)

Designation number, full name, business email address, business telephone number, function code and FAA advisor's/managing specialist's full name.

(DER)

Designation number, email address, full name, middle initial (optional), suffix (optional), company (optional), phone number, FAA advisor and mailing address (optional).

(ODA)
Designation number, representative name, representative email, company name, company city, company state, phone number, organization management team (OMT) lead, ASI OMT member and address.

(Designee Support)
Email address, full name, middle name (optional), suffix (optional), supported DER, company, phone number, and address (optional).

(Drafter)
Email address, full name, middle name (optional), suffix (optional), FAA advisor, company, phone number and address (optional).

NACIP receives the applicant's name from CPN. CPN generates a project ID to track a certification project and creates a project number. When a project number is input in NACIP, NACIP reaches out to CPN for validation. Upon validation, CPN provides NACIP with the applicant's name.

NACIP receives the designee's name, address and phone number from DMS, only if that designee has an active designation identification number.

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 the minimum amount of information from individuals to support the stated purpose of the NACIP system. NACIP uses drop-down menus to minimize selection options. It is presumed that the designee is aware of the project and knows which selections to make. The FAA has submitted a new records retention and disposition schedule National Archives and Records Administration (NARA) Aircraft Certification Service Records, N1-237-05-03 which includes documents related to specific companies or parts to include: applications, approvals, correspondence, technical data and test results, and evidence of licensing. FAA proposes to destroy the records ten years after the case is canceled, surrendered, withdrawn, or otherwise terminated.

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.

NACIP is not a Privacy Act System and shares no information with external systems. There are no other uses beyond those described in the PIA. There are approved data sharing agreements in place to govern the exchanges of information between NACIP and DMS and NACIP and CPN.

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).

Since NACIP is not the original point of collection for its data, the data that it receives is assumed to be accurate from its source. NACIP receives the applicant's name from CPN and the designee's name, address and phone number from DMS, so its accuracy of information depends on the source system.

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 the National Institute of Standards and Technology Special Publication (NIST) 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* dated September 2020 (includes updates as of December 10, 2020).

Safeguards include an annual independent risk assessment of the NACIP system to test security processes, procedures and practices. The system operates on security guidelines and standards established by NIST and only FAA personnel with a need to know are authorized to access the records in NACIP. All data in-transit is encrypted and access to electronic records is controlled by PIV cards and Personal Identification Numbers (PIN) and limited access according to job function. Additionally, the FAA conducts annual cybersecurity assessments to test and validate the security process, procedures, and posture of the system. The FAA issued NACIP the authority to operate based on the security testing and evaluation in accordance with FISMA.

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.

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

DOT implements 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.

In addition to these practices, the FAA consistently implements additional policies and procedures especially as they relate to the access, protection, retention, and destruction of PII. Federal employees/contractors who work with NACIP are given clear guidance about their duties as related to collecting, using, and processing privacy data. Guidance is provided in mandatory annual security and privacy awareness training and in FAA Order 1370.121B. The FAA also conducts periodic privacy compliance reviews of NACIP as related to the requirements of OMB Circular A-130, "*Managing Information as a Strategic Resource*."

Responsible Official

Harish Pai
System Owner
Sustainment Manager, ADE-540

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.03.26 14:34:28 -04'00'