U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Office of Security Hazardous Materials Safety (ASH)
Identity Management System (IDMS)

Responsible Official

Atul Celly
9-AWA-ASH-APPSupport@faa.gov
1-888-584-8334

Reviewing Official

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

Executive Summary

The Federal Aviation Administration (FAA) is required to meet the compliance requirements under Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, which directs the implementation of a standardized badging process for processing and issuing credentials for Personal Identity Verification (PIV) cards and identification (ID) badges. To address the requirements, the FAA Office of Security Hazardous Materials Safety (ASH) created the Identity Management System (IDMS).

The FAA is publishing the IDMS Privacy Impact Assessment (PIA) pursuant to Section 208 of the E-Government Act of 2002 because this application collects and stores personally identifiable information (PII) from members of the public, such as non-employees that need access to a FAA facility and are in the process of receiving a PIV card including FAA employees/contractors that manage the IDMS system or are new employees/contractors that are being issued a PIV card.

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:

[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).

- *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

In the past, the Federal Aviation Administration (FAA) issued Identification (ID) media that did not have the ability to store authentication information, which could then be used for system login and physical access ability. To address this issue, the Office of Security Hazardous Materials Safety (ASH) implemented the Identity Management System (IDMS), which supports identity proofing and verification, background investigation of FAA employee and contractor applicants, and PIV card issuance and maintenance.

IDMS is a web-based system that is only available within the FAA network and is not publicly accessible. IDMS collects and maintains PII from FAA employees and contractors, employees of other federal agencies, and members of the public (non-employees) (collectively called "applicants") to issue PIV/badge cards.

This PIA describes FAA's process for requesting and issuing of FAA credentials (PIV card IDs and badges) to meet the requirements under HSPD-12 and comply with the standards outlined in Federal Information Process Standards (FIPS) 201 and its accompanying special publications.

IDMS functional component:

The Card Management System (CMS), a subcomponent of IDMS, manages the status of PIV cards throughout their entire lifecycle. CMS has a data exchange with the ASH Investigation Tracking System (ITS) to pull the following applicant information from ITS: Full legal name, Date of Birth (DOB), city and country of birth, country of citizenship, i.e., United States, employee affiliation/employee type/department (e.g. Employee, Contractor, Non-Employee, Temporary), contract information (contract number and company name), ITS individual ID, ID approval status, ID approval date, escort required, and ID type (PIV or non-PIV yellow card).. This information is used to begin the PIV card initialization process for applicants. ITS provides a view for IDMS to process requests for IDs. ITS stores and maintains the official copy of these records. IDMS-CMS functions include personalizing

and printing PIV cards; activating and issuing the initial PIV card; and performing other card maintenance functions, such as re-issuance, renewal, suspension, revocation, and card media destruction. CMS also includes data for card personalization2 and information requests for PIV certificates from the public key infrastructure (PKI) Service Provider, Digicert. It also prints non-PIV employee, contractor, and temporary ID cards.

PIV Authentication Database (PAD), a subcomponent of IDMS, is the single source of identity data for PIV card usage. The data in PAD is used by Logical Access Control Systems (LACS) and Physical Access Control Systems (PACS) for fulfilling logical and physical access control business requirements. LACS enforces access control measures for systems, programs, processes, and information; PACS limits access to campuses, buildings, rooms, and physical IT assets. PAD provides other FAA internal systems, such as MyAccess and FAA Directory Services (FAA DS)/Active Directory (AD), utilize a limited view of the data from CMS, a subsystem of IDMS. Only those with a username and password can access PAD. PAD restricts access by limiting the view to specific Internet Protocol (IP) addresses.

The FAA New Hire Business Process within IDMS:

Upon completion of a favorable background investigation (this process is outside of IDMS), a newly hired applicant receives notification that they are authorized to request a FAA PIV card. They go to a service center where they must show two authorized identification documents. This link shows a listing of the acceptable forms of identification: https://www.faa.gov/sites/faa.gov/files/about/office_org/headquarters_offices/ash/AcceptableID.pdf.

Once the applicant's identification has been verified, the applicant is taken to a kiosk, where the service center specialist navigates to an internal Uniform Resource Locator (URL) and has the applicant complete the electronic FAA Form 1681 Request for PIV card. A Privacy Act Statement (PAS) is posted at the point of collection on the website and the applicant must acknowledge the PAS. Once the applicant is approved to receive their PIV card, the applicant's identity is verified, and the individual must ensure all the data elements are correct. If there is a unique match, IDMS will display the following data provided during their background investigation:

- Full Legal Name
- DOB
- City and Country of Birth
- Country of Citizenship, i.e., United States

[22] Personalization is when the PIV card is physically printed with the photo, name, employee type, expiration date, DOT seal, etc.

- Line of Business (LOB)
- Address, work mailing and physical address and home address (home address is an optional field)
- employee Type
- Contract Information
- Escort (Y/N)
- ITS Individual ID
- ID Type
- ID Approval Status and Date
- Federal Emergency Response Official (FERO) Status

Once the applicant completes the form and verifies that all the data elements are correct, they submit the request, which is routed to the designated FAA Employee Sponsor (sponsor), who reviews the request and may approve or deny the issuance of the PIV credential. If the applicant receives a denial (because they selected the wrong sponsor), the applicant is notified of the denial and can select the correct sponsor and resubmit. Once the sponsor approves, the applicant starts the enrollment process where the PIV card ID photo is taken by the service center, biometrics (fingerprints) are taken, and a Personal Identification Number (PIN) is captured and stored in IDMS. The applicant is then issued a temporary card until their new PIV card has been shipped to the facility. Once the permanent PIV card has been received at the facility, a Trusted Agent (DOT/FAA employee) updates the card status in IDMS and the applicant receives a notification that the PIV card has been delivered and they need to appear at the service center for PIV card activation.

During the activation process, the applicant must provide their biometrics and PIN they selected during their enrollment to complete the PIV card activation process. Once the PIN and biometrics are verified, the activation process writes four certificates to the applicant's PIV card chip. Upon completion of a successful activation, the Trusted Agent runs a "PIV Health Check" to verify that all required certificates are loaded, if there are any certificates missing, the Trusted Agent will redo the card activation. If everything is correct, the Trusted Agent collects and erases or destroys the temporary badge and gives the applicant their new PIV card. Once a PIV card is issued and activated, the PIV cardholder can use their PIV card to enter the requested FAA facility. The PIV card is also used to log in to the FAA network and most FAA systems (when they are authorized to access the system); some FAA systems are still in the process of implementing PIV authentication. IDMS provides the name, network log-on information (Network User ID), email address, and Digital Certificates (PIV authentication, PIV digital signing, PIV encryption, and PIV card authentication) to FAA DS/AD, which is used by these systems in performing user authentication.

PIV Card and Yellow and Orange ID Cards Request and Issuance Process:

When the FAA intends to hire a new employee or contractor the individual goes through a background investigation vetting process. Upon successful completion of a background investigation, the Personnel Security Specialist (PSS) will mark the investigated personnel record as ID Approved. The PSS also selects which type of badge can be issued.

For most applicants, this will be a PIV card. For others, i.e., (construction, cleaning crews, etc.) they may be issued a yellow or orange badge depending on the type of background investigation conducted. The applicant is notified that their badge is ready by either HR or their contracting company representative. This notification will include badging instructions.

Once the above is completed, the applicant is authorized to apply for their Identification Card using the automated 1681 application. This application only works while connected to the FAA Network or behind an FAA firewall. This application can be found by going to URL https://idms.faa.gov/1681. This is the start of the process.

All applicants must take the required training to submit the application. During the 1681 process, a training page is shown as required by FIPS 201, HSPD-12 and Digicert's registrar's practice statement. It details the responsibilities, post issuance processes, and denial of PIV and appeals process. If the applicant does not complete the training, then the information for a PIV card is not submitted to CMS. The applicant will need to take the required training and re-apply. Once training is completed, the applicant receives a confirmation email.

Once the employee reads and accepts the PAS, they enter their personal information. The employee must select their region, location within the region, last name, DOB and an email address.

The following data elements captured to initiate the application:

- Full Legal Name
- DOB
- City and Country of Birth
- Country of Citizenship, i.e., United States
- Line of Business (LOB)
- Employee Type
- Email Address

If the applicant has an existing card and needs to renew; change their name; or replace a damaged, lost, or stolen card, they select the reason.

If a sponsor declines the application, the sponsor must detail the reason during the decline process. This information is emailed to the applicant, and generally indicates why the

application was declined and what actions the applicant needs to take. Many times, it is declined because the contractor simply picked the wrong contract number or company, and the applicant just needs to fill out a 1681 again to remedy this issue.

Once the sponsor approves the application, the applicant needs to appear in person at a Service Center to complete the enrollment process (if the sponsor does not approve the request processing ends). The applicant receives an email when approved which instructs them to bring two acceptable forms of ID to the processing center. The applicant must appear at the service center to enroll for their PIV Card. After enrollment, the PIV card is ordered and arrives in five to ten days. The PIV card is shipped by Federal Express to the location selected. To fully enable the PIV card, the applicant needs to have a valid FAA email address and valid FAA network account (UPN).

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.

The FAA employs multiple techniques to ensure that individuals are informed of the purpose for which the FAA collects, uses, disseminates, and retains their PII within IDMS. A Privacy Act Statement (PAS) is posted at the point of collection and the applicant must

[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

acknowledge the PAS. Additionally, information about IDMS is provided to FAA employees and contractors via broadcast communications and email.

The FAA maintains the records in IDMS that are subject to the Privacy Act in accordance with the following Department's Published System of Records Notices (SORNs):

- DOT/ALL 9 - *Identification Media Record Systems*, 67 FR 62511 (October 7, 2002), which covers data contained in applications, photographs, all credentials/SmartCards, background investigation data [date of birth, social security number (SSN), position title and position sensitivity, assignment to sensitive duty positions, facility access, gender], biometric data including fingerprints), and personal information number (PIN)/identification and verification media password.

- DOT/ALL 13 - *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002), which covers login credentials, audit trails, and security monitoring for FAA employees and contractors who are part of the IDMS program and/or manage the system.

In addition, the publication of this PIA also demonstrates DOT's commitment to providing appropriate transparency regarding IDMS.

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.

Anyone applying for PIV Card must supply their PII and is presented with a Privacy Act Statement (PAS), for which the applicant must acknowledge before continuing to the PIV request process. Additionally, the applicant completes the form themselves and thus verifies that all the data elements are correct. Further, if a sponsor declines the application, the sponsor details the reason during the decline process. This information is then emailed to the applicant and generally indicates why the application was declined and what subsequent actions the applicant needs to take. Many times, the PIV card application is declined because the contractor simply picked the wrong contract number or company, and the applicant simply needs to fill out a 1681 again to remedy the issue.

Under the provisions of the Privacy Act, individuals wanting to contest information about their PII contained in IDMS may appear in person or may make their requests in writing, detailing the reasons why the records should be corrected. The requester must provide

suitable identification to validate their identity before a record can be changed. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Office of the Assistant Administrator for Security Hazardous Materials and Safety
Federal Aviation Administration (FAA)
800 Independence Avenue, SW
Washington, DC 20591

Included in the request must be the following:

- Name
- Mailing address
- Phone number and/or email address
- A description of the records sought, and if possible, the location of the records.

Individuals may also use the above address to register a complaint or ask a question regarding FAA's privacy practices. If you have comments, concerns, or need more information on FAA privacy practices, please contact the Privacy Division at privacy@faa.gov or 1 (888) PRI-VAC1.

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.

HSPD-12 describes the requirements for processing and issuing credentials for PIV cards and ID badges. The PII collected in IDMS is used for identity verification before issuing credentials. The FAA does not use the PII for any other purpose.

IDMS collects the following PII:

- IDMS system access and program management:
  - FAA employees and contractors: name and FAA email address.
- Issuing credentials/cards:
  - **From FAA employees and contractors**: Full legal name, DOB, city and country of birth, country of citizenship, i.e., United States, digital color photo, biometric identifiers (fingerprints), address (work mailing and physical and home), email address (work and home-home email address is an optional field), and telephone numbers, both work and

home (home number is an optional field), contract information, and Personal Identification Number (PIN).

- **From members of the public**, such as non-employees that need access to a FAA facility and are in the process of receiving a PIV card including FAA employees/contractors that manage the IDMS system or are new employees/contractors that are being issued a PIV card: Full legal name, DOB, city and country of birth, citizenship, digital color photo, biometric identifiers (fingerprints), address (work mailing and physical and home), email address (work and home-home email address is an optional field), and telephone numbers, both work and home (home number is an optional field), contract information, and PIN.

IDMS uses this information in accordance with the purposes for which it is collected under SORN DOT/ALL 9 - *Identification Media Record Systems*, 67 FR 62511(October 7, 2002), which includes to control access to DOT facilities, information or information-based systems by authenticating the identity of each person using the system.

Access and authentication records within IDMS are handled in accordance with SORN DOT/ALL 13- *Internet/Intranet Activity and Access Records*, 67 FR 30757 (May 7, 2002).

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 FAA's identity verification before processing and issuing credentials for PIV cards and ID badges. The FAA maintains different types of records in accordance with following National Archives and Record Administration (NARA) approved General Retention Schedules[5] (GRS):

- Individual's personal identification credentials and cards records are maintained temporarily, and the FAA destroys them 6 years after the end of an employee or contractor's tenure, but the FAA will keep these records for a longer period, if required for FAA's business use.[6]

- Individual's temporary and local facility identification and card access records are stored by the FAA temporarily. The FAA destroys these records once the temporary

[5] General retention schedules are used by the FAA to determine how long to maintain an individual's records and/or when to delete the individual's records and in order to promote consistent retention practices.
[6] The applicable records retention schedule is NARA GRS 5.6, approved March 2022, *Security Management Records*, Item 120 (DAA-GRS-2021-0001-005).

credential or card is returned for potential reissuance, due to nearing expiration, or within 6 months from time of issuance or when individual no longer requires access, whichever is sooner. The FAA will keep these records for a longer period if required for the FAA's business use.[7]

- Individual's information technology operations and maintenance records are temporary and are destroyed after 3 years. The FAA will keep these records for a longer period if required for the FAA's business use.[8]

- Individual's system access and audit log records are maintained in IDMS as temporary records and are destroyed when business use ceases.[9]

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 PII in IDMS is used for identity verification before processing and issuing credentials for PIV cards and ID badges from members of the public, such as non-employees that need access to a FAA facility and are in the process of receiving a PIV card including FAA employees/contractors that manage the IDMS system or are new employees/contractors that are being issued a PIV card. The FAA does not use the PII for any other purpose.

The FAA/DOT limits the scope of PII collected in IDMS to support the purpose specified in SORN DOT/ALL 9, *Identification Media Record Systems,* 67 FR 62511 (October 7, 2002). The FAA may share information with contractors for the limited purpose of assisting the Department or one of its elements in issuing, controlling and accounting for DOT identification and verification media, credentials and security badges and maintaining associated databases including contractors concerning their own current and former employees to facilitate the control and accountability of DOT identification and verification media and credential and security badges issued to contract employees.

Access and authentication records within IDMS are handled in accordance with SORN DOT/ALL 13 - Internet/Intranet Activity and Access Records, 67 FR 30757 (May 7, 2002) and are subject to the following Routine Use:

[7] The applicable records retention schedule is NARA GRS 5.6, approved March 2022, *Security Management Records*, Item 130 (DAA-GRS-2021-0001-006).
[8] The applicable records retention schedule is NARA GRS 3.1, approved January 2017, Information technology operations and maintenance records, Item 20 (DAA-GRS-2013-0005-0004).

[9] The applicable records retention schedule is NARA GRS 3.2, approved September 2014, *Information Systems Security Records*, Item 30 (DAA-GRS-2013-0006-0003).

- To contractors, grantees, experts, consultants, detailees, and other non-DOT employees performing or working on a contract, service, grant cooperative agreement, or other assignment from the Federal government, when necessary to accomplish an agency function related to this system of records.

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act systems of records, including this system. These routine uses are published in the Federal Register at 75 FR 82132, December 29, 2010, and 77 FR 42796, July 20, 2012, under "Prefatory Statement of General Routine Uses." Available at https://www.transportation.gov/individuals/privacy/privacy-act-system-records-notices.

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).

Information in IDMS is collected directly from FAA employees, contractors, and members of the public. They complete the form and verify that all the data elements are correct and thus it is assumed to be accurate. Individuals may also use the IDMS PIV card check website where the PIV cardholder may view their digital certificates, digital photo, printed information on the card and other information for accuracy. Data is encrypted in transit and at rest[10] to ensure the data is secured. In addition, to the data being provided by the individual, the data is only accepted and saved in IDMS after going through authentication, which matches the individual to their data. An FAA employee/contractor completes a review and verification of the data provided directly by the individual for accuracy before the individual submits their application.

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

[10] There are two types of data encryption. Data at-rest refers to inactive data not moving between devices or networks and tends to be stored in data archives. On the other hand, data in-transit is moving between devices or two network points.

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 Dec. 10, 2020).

These safeguards include an annual independent risk assessment of the IDMS 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 IDMS. All data in-transit and at rest is encrypted and access to electronic records is controlled by use of PIV cards, PINs, and limited according to job function. Additionally, the FAA conducts annual cybersecurity assessments to test and validate security processes, procedures and postures of the system. Based on the security testing and evaluation in accordance with the FISMA, the FAA issues IDMS an on-going authorization to operate.

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 DOT/FAA 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.

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.

In addition to these practices, the FAA will implement additional policies and procedures as needed as they relate to the access, protection, retention, and destruction of PII. Federal employees and contractors who work with IDMS 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, as well as FAA Order 1370.121B. The FAA conducts periodic privacy compliance reviews of IDMS as related to the requirements of OMB Circular A-130, *Managing Information as a Strategic Resource.*

Responsible Official

Atul Celly
System Owner
Manager, Business Services and Security Solutions Division, AXM-400

Prepared by: Barbara Stance, FAA Chief Privacy Officer

Approval and Signature

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