U.S. Department of Transportation

Privacy Impact Assessment
Federal Aviation Administration (FAA)/
Region and Center Operations (ARC)

Aeronautical Center Security Management System (ACSMS)

Responsible Official

Travis Hildebrand
System Owner
405-954-4571
Travis.Hildebrand@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: 2019.10.10 12:07:43 -04'00'

Executive Summary

The Mike Monroney Aeronautical Center (MMAC) conducts training for Federal Aviation Administration (FAA) employees and contractors and other government agencies employees, and is home to more than 8,000 full-time employees, and receives 10,000 visitors per month. The FAA developed the web-based Aeronautical Security Management System (ASMS) to allow MMAC to track the issuance of visitor passes/badges, parking decals, and keys. ACSMS collects, maintains and disseminates personally identifiable information (PII) from Federal employees, contractors, and MMAC visitors. The FAA is publishing this update to the previously published ACSMS Privacy Impact Assessment (PIA), May 10, 2010, in compliance with Section 208 of the E-Government Act of 2002 to address changes in system operations.

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.*

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.

[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).

Introduction & System Overview

The Mike Monroney Aeronautical Center (MMAC) is located in Oklahoma City and is the home to the largest number of Federal Aviation Administration (FAA) employees working outside of Washington DC. It encompasses approximately 1,100 acres and 133 buildings and is comprised of the following services:

- The Enterprise Services Center (ESC) provides information technology and financial management services to the Department of Transportation (DOT) and other federal agencies;
- The FAA Academy, provides technical training to over 87,000 students annually, conducts 2,200 classes per year and instructs 1,000 students per day; and
- The FAA Logistics Center, provides centralized maintenance, repair, and overhaul and supply chain management of the National Airspace System.

The web-based Aeronautical Security Management System (ASMS) is used by the FAA Security Force to track and issue long and short-term passes/badges for visitor's access to the MMAC; issue permanent or temporary parking decals to badged employees and visitors; and maintain an inventory of keys issued to employees and contractors for access to facilities within the MMAC.

Visitor Tracking and Badge Issuance

Visitors wanting access to the MMAC must be sponsored and require appropriate validation and approval by Security Force to gain access. ACSMS is used to tracks visitors and issue daily passes for short term visitors and long-term visitor badge.

Daily Visitor Pass

A daily visitor pass is issued to individuals who do not require access to MMAC for more than one-day, such as federal and contract employees who have forgotten or misplaced their PIV card, employee family members visiting the facility, or individuals contracted to perform a one-time service. To request a daily visitor pass, individuals report to the Visitor Center and must be sponsored and or escorted by an FAA employee or contractor who holds proper FAA credentials. The individual provides a valid U.S. picture identification such as a state driver's license that is used to confirm the individual's. The individual's name is checked against a list of individuals who are barred and not authorized to access the MMAC. Typically these individuals are employees or contractors that have separated from the MMAC or have been deemed to represent a security concern.

When an individual is barred , the responsible Division Manager notifies the Facility Manager's office who then provides the name and other physical characteristics to Security Force. The barred individuals are employees or contractors therefore; ACSMS would have collected information about them when issuing the them a parking pass, decals, or keys to a MMAC facility. Security Force access the individual's record in ACSMS and make an annotation that the employee or contractor is barred and updates the record to include the basic physical characteristics, such as height, eye color, and hair color. If the individual name is not in ACSMS, the MMAC Security Force manually enters the individual's name and the basic physical characteristics listed above.

If the individual' name appears on the barred list, security guard prohibits the visitor from entering the MMAC; however, no arrest is made. If the name is not on the list, the visitor is approved for access. The individual's name,

type of identification presented (but not the identification number), state of issuance, and expiration date are entered on to a Visitor Registration Log[2]. As part of the visitor sign-in process, the individual is required to manually enter his/her name, office visiting, time of entry and time of departure on a paper Visitor Registration Log. The sindividual is then provided a daily visitor pass that displays the word "visitor" along with the visitor's last name. The Security Force manually enters information from the Visitor Registration Log into the ACSMS at the end of each day.

Long Term Visitor Pass

Long-term visitor passes are issued to visitors (this includes temporary students, and other members of the public[3], but not DOT employees) who require temporary MMAC access for up to a six months. For a long- term visitor pass to be issued, a sponsor must submit a Visitor Request Memorandum to the Pass Identification Office (Pass and ID) and request a temporary badge for the individual. The memorandum includes the individual's name, the sponsor's name, and duration of the visit. That information is entered into ACSMS for processing. The resulting badge created includes the individual's name, the badge's expiration date and an ACSMS-generated badge number. Upon arrival, the individual is escorted to the visitor center by their sponsor. The check-in process follows the same procedures outlined above for daily visitor passes. Once the individual is validated, they are issued a badge. The issued badge has an expiration date therefore visitors are not required to return to return the badge. If they chose to return they are immediately shredded.

Parking Decals

Parking at the MMAC is available to employees, contractors and long-term visitors. The procedures for obtaining a parking decal are as follow:

Employees and Contractors Parking Decals:

Employees and contractors requiring a parking space on the MMAC must register their vehicles by completing AC Form 1600-16, Vehicle Registration.[4] The AC Form 1600-16 collects the name and signature of the vehicle owner; vehicle's year, make, type, color, license plate number, state and year of vehicle license. In addition, the form collects the employee/contractor routing symbol and phone extension of the FAA. All of this information is manually entered into ACSMS by the MMAC Security Force. Once the information has been entered into ACSMS, the Security Force reviews the driver's license to ensure identity of the person and that the license has not expired. Once the license has been verified a decal that includes a decal number is issued. This decal is required to be displayed on the vehicle windshield while parked at MMAC, as the decal number is used to track the parking space to which the individual is assigned. The decal number can also be used to identify individuals who fail to adhere to parking policy. The failure to adhere to the parking policy does not result in the issuance of a citation or fine and the instances are not accounted in ACSMS. Management is made aware of their employee's failure to adhere to policy.

[2] The Visitor Registration Log is used to track the daily visitor passes.

[3] Long-term visitors may include Construction Contractors, Commercial Delivery and Service Vendors.

[4] Access to the FAA Form 1600-16 is restricted and the form is only available on the FAA network.

Long-Term Visitors Parking Pass:

Long-term visitors submit their request for a parking pass with their initial request for access to the MMAC. Dependening on the purpose of the visit, they will need to provide applicable information. Students will need to provide the course, class number and ending date. Similarly, contractors must provide their company name and company phone number. No information pertaining to the vehicle is collected or entered into ACSMS. The individual is issued a temporary decal that includes a decal number. The decal must be displayed on their car window while the vehicle is parked at MMAC. The decal number is used to track the visitor to whom the parking space was assigned and used to identify individuals who fail to adhere to parking policy.

Physical/Electronic Key Distribution Tracking:

In order for employees and contractors to access to certain buildings or rooms, they must be provided a metal key. Other buildings or rooms are electronically managed and monitored (controlled). These buildings or rooms require a coded card key for access. Issuance of either key requires submission of AC Form 1600.6, Application for Key, to the Security Force. The Security Force manually enters the information from the form into ACSMS. The information entered includes the employee's or contractor's name, contracting Officer's Representative (COR) name and contract number if individual is a contractor, routing symbol, telephone extension, building and room number.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template 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[5], 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 [6]

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.

As described above, the FAA collects information to track the issuance of visitor passes/badges, parking decals and the issuance of keys. Individuals are made aware of the uses of the information by Security Force at the time of collection. General notice is provided to individuals through the following corresponding Privacy Act System of Records Notice: DOT/ALL 9, Identification Media Record Systems, October 7, 2002, 67 FR 62511 and DOT/FAA 807,

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

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

Traffic Control at the Mike Monroney Aeronautical Center, April 11, 2000, 65 FR 19519. This PIA further demonstrates the commitment of DOT to ensure appropriate transparency of ACSMS.

Individual Participation and Redress

DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

Individuals voluntary provide information to the FAA in order to be issued a visitor passes/badges, parking decals and the of keys. In addition, the ACSMS also include names of individuals who have been barred from accessing the facility. The information barred individuals is provided by FAA management from FAA systems and is not provided directlyfrom the individuals.

Under the provisions of the Privacy Act, individuals may request searches to determine if any records have been added that may pertain to them. Individuals wishing to know if their records appear in this system may inquire in person or in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington DC, 20591

For questions relating to DOT's Privacy Program please go to http://www.dot.gov/privacy.

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.

Contesting record procedures:

Individuals wanting to contest information about them that is contained in this system should make their requests in writing, detailing the reasons for why the records should be corrected to the following address:

Federal Aviation Administration
Privacy Office
800 Independence Ave. SW
Washington DC, 20591

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 its collects, uses, maintains, or disseminates PII.

Title 44 U.S.C. § 3101 states; "the head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions

of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities." ACSMS's purpose is to carry out such functions as vehicle registration, traffic control, access control and to maintain an orderly traffic flow on the MMAC. In addition, ACSMS provides a ready concentration of employee personal data to facilitate issuance, accountability, and recovery of required identification media issued to employees, contractors, consultants, and other individuals or personnel who require access to FAA facilities.

ACSMS collects the visitors name, type of identification, the state of issuance, and the expiration date and that information is used to validate the visitor, prevent entry of visitor that are barred from the MMAC and issue a badge. In addition, ACSMS collect the vehicle owner name and signature of the vehicle owner; vehicle's year, make, type, color, license plate number, state and year of vehicle license. The information is used to ensure the individual requesting parking has a valid driver license in order to issue a parking decal. The decal includes a number that is used to track assign parking spaces and employees who do not adhere to parking policy. Lastly, for the issuance of a metal key or an electronic (coded) key card, ACSMS collects the employee's or contractor name, routing symbol, telephone extension, building and room number, division manager signature and signature of key holder. The information is used to validate the employee or contractor and grant them access to building or room at the MMAC.

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. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule.

FAA limits the scope of PII it collects to what is necessary to track the issuance of visitor passes/badges, parking decals and keys.

For the issuance of visitor pass/badge the Security Force enters into ACSMS, the visitor's name, type of identification, the state of issuance, and the expiration date. This information is used to validate the visitor so that the Security Force may issue a visitor pass/badge. Visitor pass/badge information is retained and disposed of in accordance with National Archives and Records Administration's (NARA) General Records Schedule (GRS) 5.6 Security Records, Visitor Processing Records (Item 110). The record is destroyed when 5 years old, but longer; retention is authorized if required for business use.

Parking records are retained and disposed of in accordance with NARA's GRS 5.6 Security Records, Local facility identification and card access records (Item 130). These records are destroyed upon immediate collection once the temporary credential or card is returned for potential reissuance due to nearing expiration or not to exceed 6 months from time of issuance or when individual no longer requires access, whichever is sooner, but longer retention is authorized if required for business use.

Key and card access records are retained and disposed of in accordance with NARA's GRS 5.6 Security Records, Key and card access accountability records (Items 020 and 021). Records are destroyed 3 years or 6 months (respectively) after return of key, but longer retention is authorized if required for business use.

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.

ACSMS does not interface with other systems. For the issuance of visitor pass/badge ACSMS collects the visitor's name, type of identification, the state of issuance, and the expiration date and limits the Sharing of Privacy Act records collected, used and maintained in accordance with DOT/ALL 9, Identification Media Record Systems, October 7, 2002, 67 FR 62511. In addition to other disclosures generally permitted under 5 U.S.C. § 552a (552a (b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DOT as a routine use pursuant to 5 U.S.C. § 552a (b)(3) as follows:

- Records may be disclosed to 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.
- Records may be disclosed to Departmental contractors concerning their own current and former employees to facilitate the control and accountability of DOT identification and verification media, credential and security badges issued to contract employees.

For vehicle registration and the issuance of a decal, ACSMS collects the vehicle owner name and signature of the vehicle owner; vehicle's year, make, type, color, license plate number, state and year of vehicle license and limit that sharing in accordance with DOT/FAA 807 - Traffic Control at the Mike Monroney Aeronautical Center 65 FR 19475- April 11, 2000. There are no system specific routine use currently for this SORN.

The Department has published 14 routine uses applicable to all DOT Privacy Act SORNs, including this system. The routine uses are published in the Federal Register and are available at www.transportation.gov/privacy.

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 is manually entered into the ACSMS system from information provided on AC Form 1600-6 and AC Form 1600-16. The Security Force checks the accuracy of the information as it is entered. As badges are issued, if visitor identify inaccurate information, they have the opportunity to correct the information at that time. The system performs programmatic checks. Examples of a programmatic check would be the system will notify the security guard if the correct number of characters is not entered (zip code has five numeric spaces) and if spaces are left unfilled the system will move the cursor to the first empty space for required fields. Periodically, facility management updates and sends a list of those individuals restricted from MMAC to Division Managers.

Security

DOT shall implement administrative, technical, and physical measures 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, as revised. Security and Privacy Controls for Federal Information Systems and Organizations are managed within the ACSMS system security plan per NIST SP 800-53, as revised. The privacy control requirements as determined by the FISMA are fully described within the System Security Plan (SSP); describing Authority and Purpose (AP) of collection, Accountability, Audit, and Risk Management (AR), Data Quality and Integrity (DI) and Data Management (DM). The ACSMS was granted an Authorization to Operate (ATO) on September 13, 2018.

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 1370.121, FAA Information Security and Privacy Program and Policy provides implementation guidance for the various privacy requirements of the Privacy Act of 1974 (the Privacy Act), the E-Government Act of 2002 (Public Law 107-347), the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) mandates, NIST and other applicable DOT and FAA information and information technology management procedures.

In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to the access, protection, retention, and destruction of PII Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, and processing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Order 1370.121. The FAA will conduct periodic privacy compliance reviews of ACSMS in accordance with the requirements of OMB Circular A-130.

Responsible Official

Travis Hildebrand, AMP-300,
System Owner
Operations and Maintenance (AMP-300)

Approval and Signature

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