U.S. Department of Transportation

Privacy Impact Assessment

Federal Aviation Administration (FAA)
Office of Aviation Safety (AVS)
MyAccess / Electronic Identity Authentication Service

Responsible Official

Karyl Cooper
System Owner
Main Number: 1-866-TELL-FAA
(1-866-835-5322)

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
DN: c=US, o=U.S. Government, ou=OSTHQ, ou=DOT Headquarters, cn=CLAIRE W BARRETT
Date: 2017.05.31 13:04:27 -04'00'

Executive Summary

The MyAccess Electronic Identity Authentication (eID) Service provides identity management and authentication of non-Department of Transportation- (DOT) affiliated individuals requiring access to DOT and Federal Aviation Administration (FAA) applications on the FAA network. The eID services for MyAccess are provided through a third party service provider (IdSP).

This Privacy Impact Assessment (PIA) was developed in accordance with the E-Government Act of 2002 because the new MyAccess capabilities for identity proofing and credentialing require individuals to provide sensitive personally identifiable information (SPII). The FAA Office of Finance and Management (AFN) Office of Information and Technology Services (AIT) is accountable for the oversight and management of MyAccess.

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.

Introduction & System Overview

MyAccess is an application that identifies, validates and authenticates authorized users to access a variety of applications located on DOT's or FAA's enterprise networks.[2] Specifically, the FAA uses MyAccess to

[1] OMB's definition of the PIA is 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).

[2] MyAccess identifies, verifies and authenticates a user to the FAA environment; it does not authorize a user to login to a particular application supported by MyAccess. Application level access is determined and authorized by each specific application.

ensure a streamlined approach towards common business practices. This allows users of web-based applications to seamlessly connect, interact and respond electronically to customers, stakeholders, colleagues and resources more reliably and securely. MyAccess functionality reduces the need for passwords that would be required for accessing multiple enterprise applications on the DOT or FAA enterprise networks.

The Department has a significant business need to allow individuals external to the Department to access applications supported by MyAccess. Because these individuals have not previously had their identity verified by the Department, additional processes and information collections are necessary to ensure that individuals are who they claim to be. Given the sensitive nature of the systems accessible via MyAccess, the FAA has determined that a high degree of confidence is necessary in the validity of the identity asserted by users . To achieve this level of confidence, associated with Level of Assurance (LOA) 2 as described in the Office of Management and Budget (OMB) Memorandum 04-04, "E-Authentication Guidance for Federal Agencies,"[3] the FAA has contracted with a third-party identity proofing services provider (IdSP) to integrate that capability into MyAccess.[4] The IdSP are consistent with the National Institute of Standards and Technology (NIST) technical guidelines for federal agencies implementing remote electronic authentication of individuals interacting with government information systems (IT) systems over networks, issued in Special Publication 800-63-2, "Electronic Authentication Guideline."[5]

If the individual successfully completes the identity proofing process, the FAA receives a response from the IdSP containing the result of the authentication however, it does not receive nor store the individual's information submitted for identity-proofing purposes. When FAA receives the IdSP response, FAA creates a user account for access. The IdSP maintains a record of the Lexis Nexis ID, described in Section 8, that is generated by the transaction, which is the only data needed to establish and maintain the account and identity of the person affiliated with the account."

Electronic Identity Authentication (eID) Process

In order to have their identity electronically authenticated, users are required to register with MyAccess and create an account. Account holders may receive credentials to access the FAA network application(s) for which they are authorized. Individuals may initiate the registration and identity verification process either from the MyAccess front page, https://register.smext.faa.gov, or from the login page of the specific application to which the individual requires access. The MyAccess Registration and eID processes are conducted in real time. The following steps for registration and identity verification are applicable regardless of how the individual initiates the process:

Information Collection

The information collection for the my MyAccess Registration process for initiation of eID is conducted concurrently.

MyAccess Registration Data

1. MyAccess creates and stores a user profile that registrants can use to access MyAccess applications.
2. In order to register with MyAccess, the individual must provide the following information:

[3] https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
[4] Lexis-Nexis commercial offering for these services are identifies as "Instant Verify" and "Instant Authenticate"
[5] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

- Full name (first, last, middle, and suffix if applicable)
- Phone number (mobile or landline)
- E-mail address

Once the data is submitted, the system will generate a unique MyAccess ID for each registrant uniquely identifies each user accessing an application. The MyAccess ID attributes never change, but there may be instances when a registrant changes their email address. In these instances, the MyAccess ID is then used to distinguish and associate the changes made by the registrant.

The registration information is maintained by the FAA in the individual's MyAccess profile. When a user logs in, MyAccess sends the MyAccess ID to the FAA application.

Registration information, with the exception of the individual's email address, is also used for eID and is shared with the IdSP.

eID Data

3. Consistent with NIST requirements for remote identity verification, the IdSP must confirm that an individual is able to provide a valid, current government identification number and a financial account number established under that individual's name. In addition to the information provided for MyAccess registration, the following information is collected in order to validate an individual's identity:
   - Biographic identifiers
     - Full date of birth (month, day, year)
     - Postal mailing address
   - Government ID number
     - Social Security Number (SSN)
       OR, if SSN check fails
     - Driver's license number and issuing state
   - Financial Account Number[6]
     - Full credit card number and expiration date

This information, with the exception of the individual's SSN, is mandatory and must be provided in order for the IdSP to initiate the electronic authentication process. Neither FAA nor the IdSP store information collected for eID, with the exception of name, phone number and email address retained by the FAA as contact information.

Data Integrity and Human Check

4. MyAccess conducts a basic integrity check (for example, ensuring all mandatory fields are completed and that only numbers are entered in numeric fields) of the information provided before the data is submitted to the IdSP for verification. If the automatic check detects an error, the individual is afforded an opportunity to correct the information before it is submitted.

[6] Individual must be the "responsible party" on the account

5. In order to ensure the information is being submitted by a human being and not a machine, MyAccess has implemented security challenge-response technology intended to thwart spamming and automated input/extraction of data from the system. MyAccess may require the individual to select a particular object captured among several images (for example, to choose all images showing mountains or to enter a series of characters) to ensure that the entity providing the information is not a computer attempting to create an account.

6. Once the automated data integrity and human checks are completed, the individual is given one additional opportunity to edit the information provided before they confirm the collection and initiate the MyAccess Registration and Electronic Authentication process by clicking the "submit" button. The individual may cancel the transaction at any time before the data is submitted to the IdSP.

<u>eID</u>

7. Once an individual's information is received, the IdSP conducts a multi-layered identity verification process that includes comparing the data against trusted data sources and querying the individual to confirm additional data elements. The IdSP maintains its own unique identifying number for registrants in its records, and shares it with FAA to prevent duplication.

    a. *Data Comparison*: The IdSP uses a compilation of databases from more than 1,000 entities with whom the IdSP has entered into formal relationships for the purposes of identity-proofing. Data sources include both public (e.g. utilities, departments of motor vehicles) and proprietary information (e.g., credit card companies, cell phone providers) to identify, verify and authenticate the information submitted by the individual. If any data elements provided for eID were unable to be validated by the IdSP, the individual will be notified by MyAccess and provided an opportunity to correct or provide additional data. For example, the individual may choose to provide a different credit card. The provision of the individual's SSN number is not required, and if the individual chooses not to provide it at this stage they are afforded one additional option: to enter their driver's license number and state of issuance. If the registrant's full credit card number could not be located by the IdSP, the IdSP will verify that the registrant's name matches their supplied mobile phone number or home phone number. If a match is found, the registrant will receive a one-time personal identification number (PIN)[7] to the phone number by short message system (SMS) or with a voice call to their home phone. The registrant must enter the PIN online within 10 minutes of its issuance to continue the process.

    b. *Confirmation*: If the data comparison activity is successful, meaning that the IdSP is able to validate the individual based upon the data they provided, the individual is then asked a series of questions based on additional information available in the confirmation data set. The questions are intended to ensure that the individual submitting the information is the valid possessor of that data. For example, the individual may be asked to select a valid former residence from a list of provided addresses. If the IdSP cannot generate a suitable quiz from available data or if the user cannot answer the questions, the individual will not be able to complete the identity-proofing and MyAccess account registration process.

    The FAA does not have access to nor maintain any of the information used for or the outcomes of the eID process.

[7] A personal identification number (PIN) is a numeric password used to authenticate a user to a system.

Notification

8. The IdSP generates its own unique Lexis Nexis ID number to manage its records, and shares it with FAA to prevent duplication.
9. The individual will receive two notices that their identity has been verified; a message displayed on the screen and an email sent to the email address provided for MyAccess Registration. The email includes a link to the MyAccess website and an one-time numeric passcode which are necessary in order to complete the registration process.

Finalizing MyAccess Registration

10. The individual's registration is complete once they enter the MyAccess system using their email address and temporary passcode, create a new permanent MyAccess passcode consisting of a six- to eight-digit PIN, and choose/respond to three security questions used to help manage the account in the event that the passcode is lost or the user has other account issues. These answers are encrypted and stored by FAA within MyAccess and are not visible or accessible to anyone within the FAA. At this time the individual is also provided an opportunity to include additional information in their MyAccess profile, such as business contact information (business name, address, phone number email address) or additional personal contact information.

MyAccess only facilitates access; it does not determine a user's privileges on applications supported by MyAccess. Once the MyAccess account registration process is completed, the individual may be required to complete additional application-specific registration steps for the FAA application for which they are seeking access. These processes are not addressed in this document; however, they are addressed in application-specific PIAs as appropriate. All Departmental PIAs may be found on the Departmental Privacy Program website, www.transportation.gov/privacy.

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[8], 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[9].

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.

[8] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[9] http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

The FAA makes an effort to ensure registrants have the information to be knowledgeable of the need for the MyAccess web application and the purposes for which FAA collects, maintains, and shares PII as part of the identity proofing and MyAccess account registration processes. Individuals requiring access to a FAA application will be advised of their need to register with MyAccess to validate their identity on the takeoff page of that application.

Information provided by individuals as part of the identity-proofing process is not maintained by either the FAA or the IdSP and are therefore do not constitute records subject to the provisions of the Privacy Act of 1974. Databases used by the IdSP to validate identities – based on data provided by individuals seeking access to DOT/FAA applications protected by MyAccess – are not created at the direction of nor accessed by the FAA, and are therefore not subject to the Privacy Act. Use of these records for FAA sponsored identity-proofing activities do not constitute "matching" as defined by the Privacy Act[10] and do not constitute credit checks per the Fair Credit Reporting Act.[11]

MyAccess registration and account records are maintained in accordance with the Department's Privacy Act system of records notice note (SORN), DOT/ALL 13, *Internet/Intranet Activity and Access Records*, May 7, 2002 67 FR 30758. Accordingly, a Privacy Act Statement discussing the Department's privacy practices regarding the collection, use, sharing, maintenance, and disposal of PII is included on the homepage of the MyAccess web portal. Information maintained in the MyAccess registration records (e.g., name, mobile phone number, email address, and employer information) may be used to authenticate and verify a user's authorized access to an application supported by MyAccess.

The publication of this PIA demonstrates DOT's commitment to provide appropriate transparency into the MyAccess web application.

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.

The FAA uses the MyAccess platform to collect data directly from the individual and submit it to the IdSP for identity proofing. The IdSP compares this information against its own records and records of authoritative sources to which it has access. If the IdSP is unable to confirm the individual's initial data submission, the individual is provided an opportunity to either correct the data or provide additional data.

Individuals who choose not to provide their SSN or for whom an SSN submission cannot be verified by the IdSP may opt to provide their driver's license number. The driver's license number is not a perfect substitution for the SSN and results in less accurate identity validation outcomes, due to limitations in accessible records. Individuals whose SSN and driver's license information cannot be verified cannot complete the eID process. Similarly, individuals who provide credit card information have three opportunities to have their account information verified. If after three attempts the IdSP is unable to confirm the individual's financial information, the individual will be prompted to enter a phone number (mobile or home) to receive a one-time password. The phone number entered must match the registrant's name. If the phone number provided is not in the registrant's name the registrant will be notified that the

[10] https://www.justice.gov/opcl/privacy-act-1974
[11] https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

eID process has failed. Additionally, the individual will be unable to complete the eID process if they are unable to successfully answer the confirmation process as described above. For all of these circumstances where the eID process was not successfully complete, the individual will be notified and afforded an opportunity to complete an in-person identity validation interview and the MyAccess registration process.[12]

Neither the FAA nor the IdSP maintain data provided by the individual for identity proofing purposes and therefore do not offer processes for access or correction of this data. If the individual believes that the eID process failed due to erroneous data in the authoritative sources used by the IdSP, the individual is encouraged to contact the data owners for their specific guidelines to correct errors (e.g. contact mobile phone provider to confirm the correct name and address are on file).

In addition to aiding with identity verification, the FAA may use a registrant's email address and phone numbers to communicate with the registrant for such purposes as automating account resets or other necessary communications.

Individuals have full access to update and maintain their MyAccess profile information. Additionally, information maintained in MyAccess account registration and system access information is protected under the Privacy Act and individuals may seek access to those records. Individuals may make their inquires in person or may submit their request in writing to:

Federal Aviation Administration
Privacy Office
800 Independence Avenue (Ave), SW
Washington, DC 20591

The request must include the following information:

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

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

Federal Aviation Administration
Privacy Office
800 Independence Avenue (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.

[12] The process for in-person validation has not yet been determined in detail. This PIA will be updated as necessary once the process is formalized.

In accordance with its statutory responsibilities under the Federal Information Security Modernization Act of 2014, Public Law 113-283, 6 U.S.C. 1523(b),[13] and NIST guidance, FAA is responsible for complying with information security standards and guidelines, including minimum requirements for federal information systems (except for national security systems). NIST Special Publication (SP) 800-63-2 advises that for identity proof – to address impersonation of claimed identity – documentation that provides a specified level of confidence or assurance of the identity of the person should be used. Government-issued documents such as driver's licenses and passports are examples provided of information to be collected for identity proofing.

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.

Individuals registering accounts with MyAccess and using the eID process are responsible for the accuracy of information they provide during those processes. The data elements collected by the FAA and shared with the IdSP are the minimum necessary to comply with the NIST standards for eID. Information collected for MyAccess account registration and profile maintenance is the minimum required to establish unique accounts within the system, ensure appropriate access to applications, and maintain communications with registered individuals.

MyAccess registration profiles and records associated with the use of MyAccess to access applications will be retained and disposed of in accordance with NARA's General Records Schedule (GRS) Transmittal 26, section 3.2 ''System access records'' covering user profiles, log-in files, password files, audit trail files and extracts, system usage files, and cost-back files used to assess charges for system use. The guidance instructs, ''Destroy 6 years after password is altered or user account is terminated, 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.

Sharing of Privacy Act records collected, used and maintained as part of MyAccess registration account is done in accordance with Department SORN DOT/ALL 13, *Internet/Intranet Activity and Access Records*, May 7, 2002 67 FR 30758. In addition to other disclosures generally permitted under 5 U.S.C. § 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:

- To provide information to any person(s) authorized to assist in an approved investigation of improper access or usage of DOT computer systems.
- To an actual or potential party or his or her authorized representative for the purpose of negotiation or discussion of such matters as settlement of the case or matter, or informal discovery proceedings.

[13] Prescribing cybersecurity responsibilities for Federal agencies, including user authentication requirements.

- 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.
- To other government agencies where required by law.

The Department has published 14 additional routine uses applicable to all DOT Privacy Act SORNs, including this system. The 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 www.tranpsportation.gov/privacy.

Information collected for the eID process is not maintained by the FAA or the IdSP and is used for the limited purposes of conducting identity-proofing activities. The information in records maintained or accessed by the IdSP to validate identities is not accessible by the government and is therefore not covered by the Privacy Act.

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). Explain how data quality is ensured throughout the data lifecycle and business processes associated with the use of the data.

The FAA makes no claims that the data obtained and used for identity verification is accurate or complete. Nevertheless, if an individual believes he or she is unable to authenticate his identity due to inaccurate information accessed by the IdSP for identity proofing, the individual is advised to check their information at the various credit bureaus.[14]

The individual is responsible for the accuracy of the information they provide during MyAccess registration process. When a new user is registering, they have the opportunity to validate or edit the personal information they have entered prior to proceeding with their registration. Once MyAccess registration is complete, the individual can change their profile information as well as their security PIN and security questions as needed.

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 NIST Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013.

[14] http://www.consumer.ftc.gov/articles/0155-free-credit-reports and http://annualcreditreport.com.

MyAccess securely transmits information provided by the registrant as described in a prior section of this document to the IdSP using a secure sockets layer (SSL) connection.

FAA has a comprehensive information security program that contains management, operational, and technical safeguards that are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

- Ensure the security, integrity, and confidentiality of PII
- Protect against any reasonable anticipated threats or hazards to the security or integrity of PII
- Protect against unauthorized access to or use of PII

MyAccess was issued a three-year authority to operate (ATO) to include the integration of identity proofing on March 1, 2017.

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'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 and 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), FISMA, DOT privacy regulations, OMB mandates, and other applicable DOT and FAA information and information technology management procedures and guidance.

The permission rights to MyAccess are based upon a role-based access controls, which are granted by automation feature as managed and overseen by the FAA. In addition to these practices, additional policies and procedures will be consistently applied, especially as they relate to the protection, retention, and destruction of PII. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing privacy data. Guidance is provided in the form of mandatory annual security and privacy awareness training, as well as FAA Privacy Rules of Behavior. The DOT and FAA Privacy Offices will conduct periodic privacy compliance reviews of MyAccess with the requirements of OMB Circular A-130.

Responsible Official

Karyl Cooper
System Owner
Enterprise Search & Integration
Office of Finance and Management
Office of Information and Technology Services

Approval and Signature

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