

Supporting Statement A
[MyAccess Non-credentialed User Access Requests]
OMB 2120-XXXX

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection.

External users requesting access to FAA applications and network resources must have their identification verified prior to being provided access. An “External User” is a person who is not a credentialed federal user in possession of a Personal Identity Verification (PIV) card or a Common Access Card (CAC), and requires access via the internet to an FAA application(s).

Based upon the security level of the application(s), external users requesting access may be required to provide Personally Identifiable Information (PII) to have their identification verified. This verification process and account creation is managed by the MyAccess program.

After a requestor has had their identity verified the requestor will be required to provide further information to perform registration and account creation.

If a requestor’s ID cannot be verified at IAL2 then an account is created at the IAL1. The user may opt to contact the helpdesk via email or phone for assistance.

There is currently only one exception to this process. MyAccess provides an interface for in-person ID verification for the Pilot Records Database application. No other applications are provided with this method.

Legal and administrative requirements for the collection are defined in the following statutes, policies and guidelines:

Privacy Act Statement (5 U.S.C. Â§ 552a, as amended):

AUTHORITY: The information collected on the MyAccess External User Registration form is authorized by the Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283 , 6 U.S.C. 1523(b), and performed according to NIST Special Publication (SP) 800-63-3.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

The MyAccess program contracts with the vendor ID DataWeb to collect the minimal information necessary to verify the requestor’s identity. ID DataWeb compares the requestor’s responses to available resources such as credit reporting agencies, public records, mobile accounts and other sources. The responses are ephemeral and therefore are not stored. The collected information is only used for the purpose of verifying the identity of the user requesting access to a Federal Government application via the web.

Please address the following items specifically:

1. Whether responding to the collection is mandatory, voluntary, or required to obtain or retain a benefit.

Response to the collection of the information is required if a non-credentialed user requests access to Federal Government resources and applications.

2. Describe the entities who must respond (e.g., class 1 railroads, operators of natural gas transmission lines, etc.).

Only individual, non-credentialed users requesting access to Federal Government resources and applications must respond.

3. Whether the collection is reporting (indicate if a survey), recordkeeping, and/or disclosure.

Only statistical reporting for program accounting and MyAccess performance tracking is performed. No PII is reported on or disclosed.

4. Indicate collection frequency (e.g., bi-annual, annual, monthly, weekly, as needed).

The collection is performed only once per new, non-credentialed user account request.

5. Describe the information that would be reported, maintained in records, or disclosed (e.g., information about a hazardous materials incident including location, type of hazardous material, extent of consequences, etc.).

No reporting or disclosure is done on PII collected. Only the following information is retained for creation of the new user account:

1. Email
2. First Name
3. Last Name
4. DOB
5. Last 4 of SSN
6. Address
7. Mobile Number

6. Describe who would receive the information – DOT, first responders, the general public, etc.

Only the contracted identity verification vendor initially receives the information. Once the user's identity is verified, a subset of the data is transferred to MyAccess to be used for account creation only.

7. Succinctly describe the purpose of the collection.

The purpose of the collection is to verify the identity of a non-credentialed user requesting access to FAA applications and resources and to create an account to facilitate access.

8. If a revision, succinctly describe the revision in the Abstract and in question 15 of the Justification document.

This is not a revision.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

The information collection is automated and performed via a web site designed for that purpose. It provides for both the validation of the requesting user's identity and subsequent account creation. A user will access the desired application via a URL provided to them by the application administrators then select the registration link on that app's web page. The user will then be redirected to a MyAccess registration page. Users must pass through the specific application's web page to register. The redirection will send a user to a page similar to: <https://myaccessxtl.faa.gov>. The page may be modified per the application owner's preferences but will have the options presented on the listed URL.

Explain the basis for the decision for adopting this means of collection. Also describe any consideration you have given or are giving to the use of improved information technology to reduce the burden on the public. You must address the following:

a. Is the electronic submission of responses possible.

Yes.

b. If a form is involved, is it available for public printing off the Internet* If so, please include the url.

No. Responses are only collected via web application via fields. The required information is variable, and the responses are not retained so there is no print option provided. There is no more expedient method for collecting the information for its intended use.

c. Will the results of the information collection be made available to the public over the Internet?

No.

If the answer to any of those questions is "no", are there plans to do so? Why not? A separate aspect of the question is your use of technology. This is of particular concern in the case of interviews. Will your interviewers use laptops or other computers to directly enter the answers being provided? If not, why not?

There are no interviewers and the only method for answering questions is via web application.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purposes described in Item 2 above.

To streamline the process of user validation and account creation MyAccess has worked to ensure that the data is entered only once and is the minimum necessary to validate a requestor's identity. After the requestor's identity has been verified and the user account created there are no other data requests made.

If a user's identity cannot be verified an IAL1 account is created and the user is informed that their identity could not be verified. In this case a user may contact the help desk for assistance. Depending on the nature of the verification issue the user may be required to perform the process again however this would likely only occur due to user or system errors.

Should an existing user request access to another application(s) the application's administrators allow the specific user account access. When the user attempts to access the application the user's access is verified through the existing MyAccess account. No request for additional or redundant responses is required by MyAccess.

5. If the collection of information involves small businesses or other small entities, describe the methods used to minimize burden.

The collection does not involve requesting information from small businesses or other small entities. Response to the request for access is required of individuals requesting access to applications published by the Federal Government.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

Without proper identity validation of a non-credentialed user requesting access to Federal Government applications and resources it is not possible to securely permit access to those applications and resources. As covered by question 4 the responses are the minimum necessary to validate the requestor's identity and create an account. The responses are required only one time. It is not possible to further reduce the burden to non-credentialed users requesting access.

7. Explain any special circumstances that would cause an information collection to be conducted in a manner:

There are no special circumstances that would cause an information collection to be conducted in a manner:

- requiring respondents to report information to the agency more often than quarterly;

- requiring respondents to prepare a written response to a collection of information in fewer than 30 days after receipt of it;
- requiring respondents to submit more than an original and two copies of any document; requiring respondents to retain records, other than health, medical, government contract, grant-in-aid, or tax records, for more than three years;
- in connection with a statistical survey, that is not designed to produce valid and reliable results that can be generalized to the universe of study;
- requiring the use of a statistical data classification that has not been reviewed and approved by OMB;
- that includes a pledge of confidentiality that is not supported by authority established in statute or regulation, that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use; or
- requiring respondents to submit proprietary trade secrets, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law.

8. 60 Day Federal Register Notice:

A Federal Register Notice published on 03/17/2022 (87 FR 15487), solicited public comment. No comments were received.

No stakeholder engagement as this is a new collection.

9. Explain any decisions to provide payments or gifts to respondents, other than remuneration of contractors or grantees.

MyAccess will not provide payments or gifts to respondents.

10. Describe any assurance of confidentiality provided to respondents and the basis for assurance in statute, regulation, or agency policy.

MyAccess protects privacy information during collection using SSL-based encryption and for data transfer to the MyAccess system for account creation. ID DataWeb does not store requestor responses therefore there is not stored data to be protected. Accounts are protected by role and user based access controls within MyAccess and Active Directory in addition to using SSL for communications with users and administrators who, based on their assigned roles, may require access to user data.

MyAccess provides the following information available on the registration page in a link titled "How we protect your privacy?":

Privacy Act Statement (5 U.S.C. Â§ 552a, as amended):

AUTHORITY: The information collected on MyAccess External User Registration form is authorized by Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, 6 U.S.C. 1523(b), and NIST Special Publication (SP) 800-63-3.

PURPOSE(S): The principal purpose for the collection of the information is to create an account for individuals external to the Department of Transportation (DOT) and to allow access to web-based applications for which they are authorized. Providing your social security number (SSN) or driver's license number is optional and will not be stored/maintained by either the Federal Department of Transportation or the Federal Aviation Administration (FAA).

Routine Uses: The information collected with the exception of the SSN and driver's license number will be included in the system of records notice DOT/ALL 13 - Internet/Intranet Activity and Access Records and will be subject to the published routine uses including:

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

The Department has also published 15 additional routine uses applicable to all DOT Privacy Act system of records. These routine uses are published in the Federal Register at 84 FR 55222 - October 15, 2019 and 77 FR 42796 - July 20, 2012, and under Prefatory Statement of General Routine Uses (available at www.transportation.gov/privacy/privacyactnotices).

Disclosure: Provision of the requested information (including your social security number) is voluntary; however, failure to furnish the requested information may result in the inability of the Department to create a MyAccess account for the user.

We protect your privacy.

We only save data that we need to remember who you are and contact you. During registration we ask you for information that only you would know. We relay this information to a third-party commercial Identity Service Provider (IDSP). They use it to assure us that you really are who you claim to be, and then they throw it away. Some of this information is voluntary, but sharing it makes it more likely we can assure your identity. If we cannot confirm your identity, then we cannot provide you access.

What we do with the data new External Users enter in each field on the registration screen.

We put in your user record at FAA so that we remember who you are and can contact you.

- Name* (First, Middle, and Last)
- Phone number (mobile recommended for text message to reset password)

We ignore at FAA.

- Private-sector number in your name*

- Phone number to receive one-time passcode
- Government number*
- SSN or Driver's license
- Date of birth*

We encrypt and ask a third-party commercial Identity Service Provider (IDSP) if you are who you claim to be. They delete the data immediately.

We do not submit to the IDSP.

- Email address
- Company Name
- Job Title
- Fax
- Street Address (including city, state, ZIP)

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.

Information regarding sexual behavior, attitudes, religious beliefs, matters that are commonly considered private, or data about race or ethnicity are not relevant to non-credentialed user creation and are not collected.

12. Provide estimates of the hour burden of the collection of information. The statement should:

Summary (Annual numbers)	Reporting	Recordkeeping	Disclosure
# of Respondents	666,666.67	0	0
# of Responses per respondent	1	0	0
Time per Response	4 minutes	0	0
Total # of responses	666,666.67	0	0
Total burden (hours)	44,444.44	0	0

The estimate of the annualized time burden to the public is based on the number of respondents for the entire contracted period divided by 3 (years). The number of non-credentialed new user requests for the contract period of 3 years is 2,000,000. Each respondent is expected to spend 4 minutes, at most, to complete identity verification.

While there are no direct cost to individuals seeking to register with MyAccess, time spent could result in minor wage costs. Since respondents are expected to be a mix of FAA, non-FAA and private sector users an average wage estimate is not realistic. However, as an example non-credentialed FAA users having a median base wage for E band (GS 8 equivalent) the following is true:

E band (GS 8 equivalent) with median income of \$46,217.50 and a 40 hour work week equals \$22.22 per hour. Of that each respondent will spend approximately \$1.48 (\$22.22/60 minutes x 4 minutes). This compounds to an estimate of \$888,000.00 in total wage costs per year given an estimated ~600,000 respondents (\$1.48 x 600,000).

https://www.faa.gov/jobs/working_here/benefits/media/core_salary_with_conversion.xls

X

13. Provide an estimate for the total annual cost burden to respondents or record keepers resulting from the collection of information.

There is no Recordkeeping or Disclosure involved so there is no cost to the FAA in these areas. Further there is no cost to the individual, non-credentialed users requesting access aside from time spent, which is expected to be approximately 4 minutes.

Because this is a considered a new collection the costs do not reflect a change from past years.

14. Provide estimates of annualized costs to the Federal government. Also, provide a description of the method used to estimate cost, which should include quantification of hours, operational expenses (such as equipment, overhead, printing, and support staff), and any other expense that would not have been incurred without this collection of information.

As stated previously each response is a one-and-done. Once the account is created the user will not be required to respond again. Each response will cost the FAA \$6.00. The annualized cost over the 3 year contract period is estimated to be \$1.8 million. The cost is likely to be less but given that it is impossible to determine the exact rate at which applications may choose to integrate with MyAccess and the number of non-credentialed users that may choose to use those applications. A closer estimate is not possible.

Support costs for MyAccess are not expected to change much due to the process for creating non-credentialed user accounts being fully automated. The systems are already in place for dealing with the expected load and support costs for those systems are already covered under existing contracts.

Cost per response is \$6. For an estimated 666,666.67 annual respondents the cost per year would be \$4 million. (6\$ x 666,666.67)

15. Explain the reasons for any program changes or adjustments.

This is a new collection. There are no changes to report.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

This collection will not be published.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons why display would be inappropriate.

The date will be displayed.

18. Explain each exception to the topics of the certification statement identified in "Certification for Paperwork Reduction Act Submissions."

No exceptions.