Privacy Impact Assessment for the International Passport and Travel Tracking System (IPATTS)

April 2023

Contact Point
Jon Heal*
FAS Application Owner
(202) 720-5728

Reviewing Official
Carol Remmers*
FAS Privacy Officer
(202) 384-4487

***Original Signatures on File in Cyber Security Assessment and Management (CSAM)**

Abstract

International Passport and Travel Tracking System (IPATTS) is a web-based system that enables FAS employees, who are anticipating travel for official job duties, to quickly determine the visa requirements for their destination country or countries. Using this system, USDA employees can apply for "official" passports over the web. This PIA is being conducted as part of security assessment and authorization process.

Overview

International Passport and Travel Tracking System (IPATTS) is used by ITS to track on the preparations made for international travel. IPATTS is also used to generate reports, visa forms, USDA letters, and State Department letters. IPATTS is a web-based system that enables FAS employees to quickly determine the visa requirements for their destination country or countries. Using this system, USDA employees can apply for "official" passports over the web. The system tracks who has what passports and will keep passports until they are needed. For FAS and USDA employees and dependents to quickly determine the visa requirements for their destination country or countries. Using this system, USDA employees can apply for "official" passports over the web. The system will track who has what passports and will keep passports until they are needed.

The operation of IPATTS is mandated by 5 U.S.C. 301; 8 U.S.C. 1185, 1401 thru 1503; 18 U.S.C. 911, 1001, 1541 thru 1546; 22 U.S.C. 211a *et seq.;* E.O. 9397; E.O. 11295.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

IPATTS collects the following: Name, SSN, Date/Place of Birth, Financial Data, Health Data, Photo, and Biometric Data (fingerprints).

1.2 What are the sources of the information in the system?

Source of the information is taken from the individual.

1.3 Why is the information being collected, used, disseminated, or maintained?

IPATTS allows FAS and USDA employees and dependents to quickly determine the visa requirements for their destination country or countries. Using this system, USDA employees can apply for "official" passports over the web.

1.4 How is the information collected?

Information is collected from the individual.

1.5 How will the information be checked for accuracy?

Data entered is validated before saving it to the database. Required fields must be completed before saving to the database. Data is routinely updated/reviewed by ITS and travel coordinators.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

IPATTS data is collected under 5 U.S.C. 301; 8 U.S.C. 1185, 1401 thru 1503; 18 U.S.C. 911, 1001, 1541 thru 1546; 22 U.S.C. 211a *et seq.;* E.O. 9397; E.O. 11295.

1.7 Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The IPATTS PII is collected and must be safeguarded with adequate protections. Data is date and time stamped and only authorized users have access to the data. Data is maintained at DISC in Kansas City and has been assessed and authorized at the Moderate risk category which is sufficient for the data.

Section 2.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

IPATTS allows USDA employees and dependents to quickly determine the visa requirements for their destination country or countries. Using this system, USDA employees can apply for "official" passports over the web. The system will track who has what passports and will keep passports until they are needed.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Standard database access tools are used to access the data and to verify correctness by authorized FAS users. The vast majority of data is produced for online viewing/verification; hard copy reports can be produced. Only authorized users belonging to the specific database group can access the system. Access is determined by the database login and password.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

No commercial or publicly available data is used.

2.4 Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

All communications to/from the database is conducted using encryption. Data is also encrypted at rest. The system has been assessed and authorized to operate at the Moderate risk categorization level.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Destroy when 5 years old.
N01-0064-1987-0001 Item 701-1. (N1-64-87-1)

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes

3.3 Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

All risk associated with data retention are addressed and have been mitigated in

the System Security Plan and the Contingency Plan for the MDA/IPATTS system.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

The information is not shared.

4.2 How is the information transmitted or disclosed?

Information is not shared or disclosed within USDA

4.3 Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

N/A, there is no sharing of the data.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Data is shared with the Department if State by the production of required forms and letters for travel (passport) purposes. The PII contained in these documents is the SSN, Name, DOB, and place of birth.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes, there is a SORN, FAS-7.

https://www.usda.gov/home/privacy-policy/system-records-notices

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Sharing of the data produced by the system is with the Department of State by the production of required forms and letters for travel (passport) purposes. (Secured website)

Application level and server level safeguard and security measures are in place. The application is protected with e-auth and will not allow users to access without approval process. The server is maintained by DISC team and the backups and security measures are done by DISC.

5.4 Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The external sharing is necessary and of a benefit to the USDA personnel and adequate risk mitigation features are in place.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

Yes.

https://www.ocio.usda.gov/sites/default/files/docs/2012/FAS-7_International_Passport_and_Travel_Tracking_System.txt

6.2 Was notice provided to the individual prior to collection of information?

Yes. From the SORN:

NOTIFICATION PROCEDURE:
Individuals seeking to determine whether this system of records
contains information about themselves may submit a written request to the Privacy Act Officer, USDA/FAS/OAO, Mail Stop 1031, 1400
Independence Avenue, SW., Washington, DC 20250-1031. Individuals must specify their request regarding IPATTS inquiries.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Yes, but the employee will not be issued a passport and will not go on official travel. RECORDS ACCESS PROCEDURE:
Individuals who request access to or amend records pertaining themselves should contact the Director, International Travel, USDA/FAS/OFSO/IS, Mail Stop 1061, 1400 Independence Avenue, SW., Washington, DC 20250-1061

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No, its all or none. The user can refuse but then they will not get the passport and will not be allowed to go on travel.

6.5 Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Data collection is done with the active participation of the individual only after being notified. Data cannot be collected without them being aware of the collection.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals can access to their data using the procedures identified in the SORN and the privacy notification.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Users can correct any inaccurate data using the procedures identified in the SORN and the privacy notification.

7.3 How are individuals notified of the procedures for correcting their information?

Users can correct any inaccurate data using the procedures identified in the SORN and the privacy notification when the data was collected.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Contact information is provided with the privacy notification and SORN.

7.5 Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There is minimal privacy risk regarding availability of redress. Individuals are provided redress procedures when the data is collected.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

All FAS/MDA personnel with access to the system are screened in accordance with USDA personnel procedures and are only allowed access after Information Security Awareness (ISA) training and signing specific rules of behavior.

8.2 Will Department contractors have access to the system?

Yes.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Users are provided annual Information Security Awareness (ISA) training which has a privacy component. Users with specific security related positions are provided role based training. The FAS Travel Office provides the necessary training to IPATTS users.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The MDA/IPATTS system has been certified and accredited for operation including adequate security auditing procedures and technical safeguards to prevent misuse of data.

The auditing is done by USDA Headquarters, International Travel Section by manual review and information captured in the database to generate audit reports. The technical safeguards are the application level and server level safeguard and security measures (Provided by DISC). The application is protected with e-auth and will not allow users to access without approval process.

8.6 Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy risks were identified and mitigated as part of the C&A process for MDA/IPATTS. The system does collect PII data and the primary privacy risks (undesired access/release) are mitigated by requiring e-Authentication account access and operating the system in the secure USDA DISC environment.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

Visa/travel support

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Technology being used is state of the practice information technology.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

N/A, this is not a 3rd party system.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

None.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A, data is not available through a 3rd party website/application.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A, data is not available through a 3rd party website/application.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A, data is not available through a 3rd party website/application.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A, data is not available through a 3rd party website/application.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A, data is not available through a 3rd party website/application.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A, data is not available through a 3rd party website/application.

10.10 Does the system use web measurement and customization technology?

The system does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

The system does not use web measurement and customization technology.

10.12 Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A, data is not available through a 3rd party website/application.