Privacy Impact Assessment

Marketing Development and Administration (MDA)

TFAA

- Version: 2.0
- Date: May 2021
- FAS-Combined PIA for MDA Child Systems
- DAIRIES, IAFTS, IPATTS, iMART, FSOAS and FSOBS

Privacy Impact Assessment for the

Dairy Accelerated Importer Retrieval and Information Exchange System (DAIRIES)

May 2021

Contact Point
Jon Heal
(202) 720-5728

Reviewing Official
Carol Remmers
FAS Privacy Officer
United States Department of Agriculture
(202) 720-2369

Abstract

The Dairy Accelerated Importer Retrieval and Information Exchange System (DAIRIES) through the Dairy Import Quota Program issues import licenses to administer the TRQ (tariff-rate quota) system for U.S. imports of dairy products. Import licensing is one of the tools USDA uses to administer the tariff-rate quota system for U.S. imports of dairy products. This PIA is being conducted as part of security assessment and authorization process.

Overview

Importers, exporters and manufacturers access the FAS Market Development and Administration (MDA) Dairy Accelerated Importer Retrieval and Information Exchange System (DAIRIES) web-based application to obtain import licenses, to check the status of license information, and to verify their license usage. The Dairy Program Office accesses the client-server application to review and verify license information submitted by users from the DAIRIES web-based application. In order for importers to apply for, receive and monitor their dairy import licenses through DAIRIES, they must have a U.S. Customs and Border Protection (Customs) importer number, which is either a Taxpayer Identification Number (TIN) or a social security number. Importers must meet required annual minimum import amounts in order to be eligible to apply for a license. The Dairy Import Licensing Group must verify importer eligibility, and can only do so by accessing the importer's Customs record using the Customs importer number.

DAIRIES contains individual dairy import license and application information which includes the following: company name, address, telephone number, fax number, point-of- contact, agent name, email address, IRS number (TIN), and ownership information. The system uses no employee or other information.

The operation of DAIRIES is mandated by Federal Regulation: Code of Federal Regulations TITLE 7—AGRICULTURE PART 6 -- Subpart--Dairy Tariff-Rate Import Quota Licensing Import licensing is one of the tools the U.S. Department of Agriculture (USDA) uses to administer the tariff-rate quota (TRQ) system for U.S. imports of dairy products.

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?

DAIRIES collects the following: company name, address, telephone number, fax

number, point-of-contact, agent name, email address, IRS number (TIN), and ownership information. The system uses no employee or other information

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

Source of the information is taken from the individual and U.S. Customs and Border Protection.

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

The Dairy Import Licensing Group must verify importer eligibility, and can only do so by accessing the importer's Customs record using the Customs importer number.

1.4 How is the information collected?

Information is collected from the individual and U.S. Customs and Border Protection. Individual importers submit their information using DAIRIES. The Dairy Import Licensing Group verifies the information in DAIRIES with U.S. Customs and Border Protection.

1.5 How will the information be checked for accuracy?

The data is verified with data from U.S. Customs and Border Protection. Data will be cross- referenced with Customs using IRS number (TIN), and by reviewing notary statements reflecting accurate verification of customer.

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

The operation of DAIRIES is mandated by Federal Regulation: Code of Federal Regulations TITLE 7—AGRICULTURE PART 6 -- Subpart--Dairy Tariff-Rate Import Quota Licensing Import licensing is one of the tools the U.S. Department of Agriculture (USDA) uses to administer the tariff-rate quota (TRQ) system for U.S. imports of dairy products.

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

DAIRIES collects the following: company name, address, telephone number, fax number, point-of-contact, agent name, email address, IRS number (TIN), and ownership information. The system uses no employee or other information. 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 delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The Dairy Import Licensing Group must verify importer eligibility, and can only do so by accessing the importer's Customs record using the Customs importer number.

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

Standard SQL database access tools are used to access the data and to verify that an Importer is eligible. The vast majority of data is produced for online viewing/verification; hard copy reports can be produced.

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 Privacy Impact Analysis: 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?

Records are maintained for a minimum of 1 year as defined by NARA records

management policy. System backup and storage of the data is provided by DISC consistent with NARA and USDA policy for data retention.

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

The DAIRIES system, as child system of the MDA System, has undergone a Moderate level assessment and authorization process and consistent with FISMA, NIST, NARA, and USDA guidelines and has been authorized to operate at the Moderate system categorization level.

3.3 Privacy Impact Analysis: 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/DAIRIES 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 Privacy Impact Analysis: 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 not shared with external organizations. Users have access only to their data using their assigned control number and their registered eAuthentication account.

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.

N/A

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 outside the scope of the automated system.

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

N/A

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_8_Dairy_Accelerated_Importer_Retrieval_and_Information_Exchange_System.txt

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

Yes, notice was published in the Federal Register, Vol. 73, No. 89 on Wednesday, May 7, 2008.

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

Yes, it is stated in the Federal Register, Vol. 73, No. 89 on Wednesday, May 7, 2008 that importers must provide the Dairy Import Licensing Group with specific information in order to apply for a license. If importers do not want to apply for a license, they do not have to provide any information.

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

The individuals can consent to the use of the data to verify their existence as an importer. The individual can decide not to provide the data.

6.5 Privacy Impact Analysis: 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 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 have online access to their own data using their assigned control number and their registered eAuthentication account.

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

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

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

Users have an edit capability and are also given notice of their ability to correct the data.

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

Contact information is provided with the privacy notification.

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

With online access to their data and available privacy officer contact information there is minimal privacy risk regarding availability of redress.

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 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 security awareness training and users with specific security related positions are provided role based training.

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/DAIRIES system has been certified and accredited for operation including adequate security auditing procedures and technical safeguards to prevent misuse of data. Technically, DAIRIES system is integrated with USDA eAuthentication software which requires all users of DAIRIES to have an eAuthentication account. The technical safeguards are the application level and server level safeguard and security measures (Provided by D I S C). The application is protected with eauth and will not allow users to access without approval process.

8.6 Privacy Impact Analysis: 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/DAIRIES. The system does collect PII data and the primary privacy risks (undesired access) are mitigated by requiring eAuthentication 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?

Import Licensing

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

DAIRIES does not employ any technology that would raise privacy concerns.

Additionally, FAS has an active Configuration Control Board (CCB) which meets every Tuesday to discuss all system changes, updates/upgrades and modifications. If new technology were needed for DAIRIES or any MDA component, it would have to be completely vetted by the FAS CCB.

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?

No

10.12 Privacy Impact Analysis: 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.

Privacy Impact Assessment for the

International Activities and Financial Tracking System (IAFTS)

May 2021

Contact Point
Jon Heal
FAS
(202) 720-5728

Reviewing Official
Carol Remmers
FAS Privacy Officer
United States Department of Agriculture
(202) 720-2369

Abstract

The Marketing Development and Administration's (MDA) International Activities and Financial Tracking System (IAFTS) is utilized primarily by the Office of Capacity Building and Development (OCBD), the Office of Country and Regional Affairs (OCRA) and the Contracts and Agreements Division (CAD) of the Office of Administrative Operations (OAO) to track USDA's overseas projects and activities from both the financial aspect (Financial), as well as the programmatic (narrative) aspect of projects. This PIA is being conducted as part of security assessment and authorization process.

Overview

The International Activities and Financial Tracking System (IAFTS) system is a major tool in providing FAS with accurate and detailed data to efficiently manage activities and fiscal operations. IAFTS data is used to pay personnel for services rendered, as well as for several basic reports. IAFTS also provides the Agency with the tools to manage and report reimbursable activity of the Agency.

Users of the system include the Financial Management Division (FMD) employees, employees of FAS's program staff, employees of the FAS Budget Division, and provides support to personnel in the Farm Service Agency. Indexing is done on last name, first name. The operation of IAFTS is mandated by Federal Regulation: Code of Federal Regulations TITLE 7—AGRICULTURE PART 6.

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?

IAFTS collects the following: Federal employee's, private citizen's and foreign visitor's data included in the records are name, address, birth city, birth country, date of birth, email address, and phone number.

SSN is not collected in IAFTS. SSN is not fed from another system.

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

Source of the information is taken from the individual by written correspondence and manually entered in IAFTS by FAS Program Areas users

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

The IAFTS data is used to keep track of personnel for services rendered, as well as for several basic reports. IAFTS also provides the Agency with the tools to manage and report reimbursable activity of the Agency.

1.4 How is the information collected?

Information is collected from the individual. Individual information is received by the FAS Program Areas either through attachments in an email or by postal services.

1.5 How will the information be checked for accuracy?

The data is verified by automated edit checks, reviewed by certified officers.

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

The operation of IAFTS is mandated by Federal Regulation: Code of Federal Regulations TITLE 7—AGRICULTURE PART 6.

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

IAFTS collects federal employee's, private citizen's and foreign visitor's data included in the records are name, address, birth city, birth country, date of birth, email address, and phone number. 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 delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

IAFTS data will be used to pay personnel for services rendered, as well as for several basic reports. IAFTS also provides the Agency with the tools to manage and report reimbursable activity of the Agency.

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

Standard SQL database access tools are used to input and access the data. The vast majority of data is produced for online viewing; hard copy reports can be produced.

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 Privacy Impact Analysis: 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 are 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?

Records are maintained for a minimum of 1 year as defined by NARA records management policy. System backup and storage of the data is provided by DISC consistent with NARA and USDA policy for data retention.

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

The IAFTS system, as child system of the MDA System, has undergone a Moderate level assessment and authorization process and consistent with FISMA, NIST, NARA, and USDA guidelines and has been authorized to operate at the Moderate system categorization level.

3.3 Privacy Impact Analysis: 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/IAFTS 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 Privacy Impact Analysis: 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 not shared with external organizations. Users have access only to their data using their assigned control number and their registered eAuthentication account.

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.

N/A

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 outside the scope of the automated system.

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

N/A

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.

SORN not published

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

Yes

The system is a major tool in providing FAS with accurate and detailed data to efficiently manage activities and fiscal operations. IAFTS data will be used to pay personnel for services rendered, as well as for several basic reports. IAFTS also provides the Agency with the tools to manage and report reimbursable activity of the Agency.

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

Yes

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

The individuals can consent to the use of the data. The individual can decide not to provide the data.

6.5 Privacy Impact Analysis: 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 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 their data in accordance with the privacy notification.

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

Users can correct any inaccurate data by notifying their FAS Program Area point of contact (POC) The POC will then manually go into IAFTS to make corrections.

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

Users are given notice of their ability to correct the data when they initially provide the data.

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

Contact information is provided with the privacy notification.

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

With available privacy officer contact information there is minimal privacy risk regarding availability of redress.

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 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 security awareness training and users with specific security related positions are provided role based training.

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/IAFTS system has been certified and accredited for operation including adequate security auditing procedures and technical safeguards to prevent misuse of data. Technically, IAFTS system is integrated with USDA eAuthentication software which requires all users of IAFTS to have an eAuthentication account. IAFTS software validates the eAuthentication account to confirm user has access. . The technical safeguards are the application level and server level safeguard and security measures (Provided by DISC).

8.6 <u>Privacy Impact Analysis</u>: 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 the system. The system does collect PII data and the primary privacy risks (undesired access) are mitigated by requiring eAuthentication 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?

Managing international and domestic activities.

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

IAFTS does not employ any technology that would raise privacy concerns.

Additionally, FAS has an active Configuration Control Board (CCB) which meets every Tuesday to discuss all system changes, updates/upgrades and modifications. If new technology were needed for IAFTS or any MDA component, it would have to be completely vetted by the FAS CCB.

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?

To engage openly with the public

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?

No

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 Privacy Impact Analysis: 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.

Privacy Impact Assessment for the

International Passport and Travel Tracking System (IPATTS)

May 2021

Contact Point
Jon Heal
FAS
(202) 720-5728

Reviewing Official
Carol Remmers
FAS Privacy Officer
United States Department of Agriculture
(202) 720-2369

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 have to 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 Privacy Impact Analysis: 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 delineate clearly 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 Privacy Impact Analysis: 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?

Records are maintained for at least 15 years - trip and passport data older than 15 years after expiration can be deleted.. System backup and storage of the data is provided by DISC consistent with NARA and USDA policy for data retention.

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

The IPATTS system, as child system of the MDA System, has undergone a Moderate level assessment and authorization process and consistent with FISMA, NIST, NARA, and USDA guidelines and has been authorized to operate at the Moderate system categorization level.

3.3 Privacy Impact Analysis: 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 Privacy Impact Analysis: 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.

FAS-7.

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 eauth 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 Privacy Impact Analysis: 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 Privacy Impact Analysis: 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 Privacy Impact Analysis: 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 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 security awareness training and 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 eauth and will not allow users to access without approval process.

8.6 Privacy Impact Analysis: 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 eAuthentication 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 Privacy Impact Analysis: 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.

Privacy Impact Assessment for the

Integrated Management Administrative Resource Tool System (iMART)

May 2021

Contact Point

Jon Heal
FAS
(202) 720-5728

Reviewing Official

Carol Remmers
FAS Privacy Officer
United States Department of Agriculture
202 720-2369

Abstract

The Marketing Development and Administration's (MDA) Integrated Management and Resources Tool System (iMART) includes an Integrated Financial Accounting Systems (iFAS) and Global Employment Management System (GEMS) . These systems will enable FAS to migrate from current manual processes to automated processes for a variety of activities.. This PIA is being conducted as part of security assessment and authorization process.

Overview

The Integrated Management and Resources Tool System (iMART) is a major tool in providing FAS with accurate and detailed data to efficiently manage activities and fiscal operations. iMART data is used to track & locate personnel transactions. iMART consists of sub-systems:

- Integrated Financial Accountability System (iFAS), shall provide FAS with the ability to track, review, approve, and reconcile expenditures at Posts.

- Global Employment Management System (GEMS) shall provide comprehensive employment data for all overseas FAS headquarters employees. Application shall track and locate personnel transactions.

Users of the system include the Office of the Chief Operating Officer (OCOO) Budget Division Employee, Office of Foreign Services Operation (OFSO), Office of Agreements and Scientific Affairs (OASA), Office of trade Program (OTP), Office of Capacity Building and Development (OCDB) and USDA APHIS Employees.

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?

iMART collects the following information:

1) Personnel data - includes name, block/vendor number, address, sex, citizenship, date and place of birth, marital status, and the names and birth dates of eligible family members;
2) Career data - includes education level, college(s) attended, major subjects, skill codes, foreign language training and examination scores, time in class, and time in service;
3) Job history data - includes both current and previous position titles, pay plans, grades, assignment dates, locations, and pending assignment information; and
4) Organizational data - includes organizational hierarchies, accounting information, awards, disciplinary actions, space requirements, etc.
5) Budget & Financial Data – includes Payroll and expenditures at oversea post office.

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

Source of the information is taken from NFC, FMMI, Global Foreign Affairs Compensation System, Department of State Payroll System (EAPS) and Department of State COASTS Data.

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

iMART (Integrated Management Administrative Resource Tool) use the information to:

- Support the mission of FAS by facilitating the sharing and flow of information (Global Sharing).

- Enterprise platform that automates and synchronizes business processes for HQ & Overseas operations.
- Provide one-stop-shopping for all HR and financial activities.
- Reduce the amount of time required to enter and manipulate data, and gives budget analyst more time to use and analyze it.

1.4 How is the information collected?

Information is collected from the report and/or spreadsheet provide by Global Foreign Affairs Compensation System ,NFC, FMMI, EAPS and COAST.

1.5 How will the information be checked for accuracy?

The data is verified by automated edit checks, reviewed by certified officers.

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

The operation of iMART is mandated by Federal Regulation: Code of Federal Regulations TITLE 7—AGRICULTURE PART 6.

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

iMART collects federal employee's, private citizens and foreign visitor's data included in the records are name, address, birth city, birth country, date of birth, email address, and phone number. 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 are 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 delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

iMART Data uses for:

- streamline budgeting and accounting practices across Program Areas
- linkage of financial data to HR data by position and employee
- provide greater accountability of expenditures of funds
- facilitate the complex reconciliation process of financial data from USDA and DOS accounting systems and the multiple payment systems
- reduce the number of auxiliary systems used to process expenditures

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

Standard SQL database access tools are used to input and access the data. The vast majority of data is produced for online viewing; hard copy reports can be produced.

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 Privacy Impact Analysis: 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?

Records are maintained for a minimum of 1 year as defined by NARA records management policy. System backup and storage of the data is provided by DISC consistent with NARA and USDA policy for data retention.

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

The iMART system, as child system of the MDA System, has undergone a Moderate level assessment and authorization process and consistent with FISMA, NIST, NARA, and USDA guidelines and has been authorized to operate at the Moderate system categorization level.

3.3 Privacy Impact Analysis: 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/iMART 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 transmitted by e-mail within USDA.

4.3 Privacy Impact Analysis: 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 not shared with external organizations. Users have access only to their data using their assigned control number and their registered eAuthentication account.

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.

N/A

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 outside the scope of the automated system.

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

N/A

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, 2019-25020, Integrated Management Administrative Resources Tool System (iMART). USDA/FAS–9.
https://www.federalregister.gov/documents/2019/11/19/2019-25020/privacy-act-of-1974-new-system-of-records

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

Yes

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

N/A

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

N/A

6.5 Privacy Impact Analysis: 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 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 their data in accordance with the privacy notification.

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

Users can correct any inaccurate data by notifying their FAS Program Area point of contact (POC). The POC will then manually go into iMART to make corrections.

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

Users are given notice of their ability to correct the data when they initially provide the data.

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

Contact information is provided with the privacy notification.

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

With available privacy officer contact information there is minimal privacy risk regarding availability of redress.

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 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 security awareness training and users with specific security related positions are provided role based training.

8.4 Has A+A 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/iMART system has undergone the RMF process for operation including adequate security auditing procedures and technical safeguards to prevent misuse of data. Technically,

iMART system is integrated with USDA eAuthentication software which requires all users of iMART to have an eAuthentication account. iMART software validates the eAuthentication account to confirm the user has access. The technical safeguards are the application level and server level safeguard and security measures (Provided by DISC).

8.6 Privacy Impact Analysis: 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 A&A process for the system. The system does collect PII data and the primary privacy risks (undesired access) are mitigated by requiring eAuthentication 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?

Management Administrative & Financial System

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

iMART does not employ any technology that would raise privacy concerns.
Additionally, FAS has an active Configuration Control Board (CCB) which meets every Wednesday to discuss all system changes, updates/upgrades and modifications. If new technology were needed for iMART or any MDA component, it would have to be completely vetted by the FAS CCB.

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

10.3 What personally identifiable information (PII) will become 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.

10.4 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 of all uses of web measurement and customization technology?
No

10.12 Privacy Impact Analysis: 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.

Privacy Impact Assessment for the

Foreign Service Officer Appraisal System (FSOAS)

May 2021

Contact Point

Truc Dao Nguyen
Project Manager
United States Department of Agriculture
(202) 690-3358

Reviewing Official

Carol Remmers
FAS Privacy Officer
United States Department of Agriculture
(202) 720-2369

Abstract

The Foreign Service Officer Appraisal System (FSOAS) is a web-based application with e-Authentication integration used by Foreign Agricultural Service (FAS) Foreign Service Officers (FSOs) to document their yearly performance, including: performance elements, accomplishments. FAS Office of Foreign Affairs uses the system to rate FSOs and FSOs can also comment on ratings within the system. This PIA is being conducted as part of security assessment and authorization process.

Overview

Foreign Service Officer Appraisal System (FSOAS) is used by FAS Foreign Service Officers posted overseas. FSOAS is owned by FAS. Foreign Service Officers are required to go through a yearly performance appraisal, and they use the "FSO Appraisal" system to submit their self-appraisal data. Appraisal data once submitted is reviewed and commented upon, by the FSO's first- and second-line supervisors. That information is further validated by the Agency's HR personnel. Once the annual appraisal round is over, the collected information is formatted as pdf documents and given to the FAS Program Office, Foreign Affairs (FA) performance appraisal committee for further consideration on FSOs' promotion related matters.

Section 1.0 Characterization of the Information

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

The Foreign Service Officers of the FAS posted overseas need to go through a yearly performance appraisal, and they use the "FSO Appraisal" system to submit their self-appraisal data. Appraisal data once submitted is reviewed and commented upon, by the FSO's first- and second-line supervisors. That information is further validated by the Agency's HR personnel. Once the annual appraisal round is over, the collected information is formatted as pdf documents and given to the FAS Foreign Affairs Office performance appraisal committee for further consideration on FSOs' promotion related matters.

The collected information contains Foreign Service Officer's Accomplishment statement, the performance elements against which the employee's performance is rated, employee's rater statement, employee's reviewer comments, HR comments if any and citations, Awards and Chief of Mission statements in pdf and word documents formats.

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

The application database is initialized with lookup data related to Position titles, Duty Stations, Position Grades and Appraisal Period dates. All other appraisal related data is directly gathered by various actors in the system.

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

The data collected by the system is used primarily to evaluate the Foreign Service Officer's job performance leading to the employee's promotion related matters. This exercise is done on an annual basis every year.

1.4 How is the information collected?

The information is collected through the data entry form within the application. The information is typed in directly by the users of the system. Citations, Awards and Chief of Mission statements are uploaded as PDF and Word documents into the system.

1.5 How will the information be checked for accuracy?

FSO's self-appraisal is verified for factual correctness by their first and second line supervisors and check for legal correctness by the HR personnel.

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

N/A

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

The requirements of the application demand that no privacy related data is needed to meet the application's stated goals. Whenever any such data gets into the system, HR personnel gets involved, and work with the users of the system, so that privacy related data could be purged. The application is also protected by e-Authentication system, to limit access to only those that have OFSO approved accounts. E-Auth level roles are being used to grant access to admin level roles.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The data collected by the application is used by FAS Program Area Foreign Affairs Performance Evaluation board as a basis for deciding promotion related matters.

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

The data collected by the application is reproduced as a printable PDF documents for further manual analysis by the OFSO management council (Performance evaluation board).

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

The system does not use any commercial or publicly available data.

2.4 Privacy Impact Analysis: 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. 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?

Records are maintained for a minimum of 1 year as defined by NARA records management policy. System backup and storage of the data is provided by DISC consistent with NARA and USDA policy for data retention.

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

The FSOAS system, as child system of the MDA System, has undergone a Moderate level assessment and authorization process and consistent with FISMA, NIST, NARA, and USDA guidelines and has been authorized to operate at the Moderate system categorization level.

3.3 Privacy Impact Analysis: 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/FSOAS 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 collected is shared with OFSO/FAS. Information shared is the self-appraisal of the FSO's along with the rater and reviewer's comments and Citations, Awards and Chief of Mission Statement documents that were uploaded into the system by the Foreign Service Officers

4.2 How is the information transmitted or disclosed?

The collected information is formatted and printed onto FAS-436 form in PDF format, one pdf document per employee. FAS HR personnel is responsible for this printing activity, as they have to signoff on the collected data before submitting the PSD documents to the OFSO performance evaluation board.

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

The internal information sharing process is an offline process that involves formatting and printing the data on to FAS-436 form, and so is outside the scope of the system, as far as mitigating the risks are considered.

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?

The data from Appraisal system is not shared with any organizations external to the agency.

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.

N/A

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

N/A

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

N/A

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.

No, it does not require a SORN

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

N/A

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

The employees are generally expected to provide the self-appraisal information and sign and date it, but they have the option of not signing it. In the event they don't want to sign, they need to provide the reason for not signing it.

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

The application requires that the Foreign Service Officers, Raters and Reviewers sign and date the section where they enter the data. The Signature applied by the users is used as a means of user consent for the use of data by the performance evaluation board.

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

Before the start of the appraisal cycle, FAS OFSO sends out a circular to the overseas posts informing the Foreign service employees about the upcoming appraisal cycle.

Section 7.0 Access, Redress and Correction

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

Any attempt to login to the system by unauthorized users will be put into a registration queue and an email is generated and sent to OFSO by the system. Designated OFSO employee then approves (or rejects) queued requests by logging into the system and activating the user accounts.

In addition to the account activation, privileged accounts such as Application Admins and HR accounts need to be assigned e-Auth level roles.

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

When the collected data is deemed erroneous or inaccurate by the Raters, Reviewers or HR, a built-in workflow within the application is used to reverted control back to the appropriate users for data correction.

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

The individuals are notified via application generated email, in addition to HR/Rater/Application support personnel manually reaching out to them.

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

The process is managed within OFSO.

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

With available privacy officer contact information there is minimal privacy risk regarding availability of redress.

Section 8.0 Technical Access and Security

.

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

Application is protected by USDA e-Auth system, and user account activation is controlled within the application. A formal email request by the application stakeholders (FAS/OFSO) is required to activate the user's account. Same process is used for user account deactivation. Upon reception of the formal request, application admins will carry out the account activation/deactivation process.

8.2 Will Department contractors have access to the system?

Yes. They perform the application look up data maintenance and general administration activities. The access is limited to 1 or 2 contractors.

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

Users are provided annual security awareness training and users with specific security related positions are provided role based privacy training (located in AgLearn).

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

Yes, for the accreditation boundary, Market Development and Administration (MDA).

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

The application is accessible only by the authorized users and is being logged by the application. All changes to the data are also captured with the user that made the change. Only authenticated and activated users (limited to OFSO/FAS and FAS HR) is allowed access to the system. Privileged access to roles such as Admins, Area directors and HR is further controlled by e-Auth level role assignment.

8.6 Privacy Impact Analysis: 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 A&A process for the system. The system does collect PII data and the primary privacy risks (undesired access) are mitigated by requiring eAuthentication account access and operating the system in the secure USDA DISC environment.

Section 9.0 Technology

9.1 What type of project is the program or system?

Appraisal system is a web application implemented using Microsoft Dotnet framework and Microsoft SQL Server. The application uses USDA e-Authentication system to authenticate and authorize users. The system runs on hardware provided by DISC and runs on Microsoft Windows 2016 Operating system.

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

The system is not using any technology that may raise privacy concerns. Additionally, FAS has an active Configuration Control Board (CCB) which meets every Wednesday to discuss all system changes, updates/upgrades and modifications. If new technology were needed for FSOAS or any MDA component, it would have to be completely vetted by the FAS CCB.

Section 10.0 Third Party Websites/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?

This system does not use any third party websites or applications.

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

Since the system does not use any third party websites or applications, there is no impact on PII.

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

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

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

N/A

If so, is it done automatically?

N/A

If so, is it done on a recurring basis?

N/A

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

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

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

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Not Applicable

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?

Not Applicable

10.12 <u>Privacy Impact Analysis</u>: 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

Privacy Impact Assessment for the

Foreign Service Officer Bidding System (FSOBS)

May 2021

Contact Point

Truc Dao Nguyen
Project Manager
United States Department of Agriculture
(202) 690-3358

Reviewing Official

Carol Remmers
FAS Privacy Officer
United States Department of Agriculture
(202) 720-2369

Abstract

The Foreign Service Officer Bidding System (FSOBS) is used by Foreign Service Officers (FSO) when they transition from overseas posts, their previous positions become open for bidding. Bidding is held in several rounds. The FSOBS provides a web-based e-Authentication platform to create bidding rounds, and enter and manage bids for post positions. This PIA is being conducted as part of security assessment and authorization process.

Overview

The foreign Service Act of 1980 sets out certain requirements for the Career Foreign Service Officers in terms of their Domestic and Overseas Tour of Duty. As per those terms, the FSOs have 2 to 5-year limit on their current Overseas assignments before they need to be rotated out to either another overseas post or to a domestic assignment. This rotational onward assignments for officers are determined through a bidding-and-paneling process that culminates with an assignment. The objective of the process is to assign officers to positions for which they are qualified and available, in reasonable anticipation of vacancies, in a manner that is responsive to the needs of the Service and considers the career needs and personal preferences of the officers. The online application used for this purpose is called "FSO Bidding" Application.

The FSO Bidding application requires the biographical information of the bidding Foreign Service Officer, along with their Position preference and a supplemental statement for a successful bid round. The biographical information such as the bidder's current position and post, their foreign language scores, previous assignments, educational qualification and citation and awards. The source of this data is the agency's iMART application and is being programmatically shared with the FSO bidding application. The bid preference and the supplemental statement is directly entered into the system by the bidder.

Typically, the main bid round is opened in the system during the fall season of the year, and additionally 1 or 2 "mini-bid rounds" are conducted to fill all overseas and domestic positions that were not assigned during the main round. The bidding process is concluded, when the OFSO committee meets and issues their position placement recommendations to the agency.

The bidding application is a web application developed using Microsoft Dot Net framework and is deployed on Windows Operating system hosted in DISC managed data center. It uses SQL Server for the data store and Department's e-Authentication system for Identity and authorization. The User interface of the application is developed using Angular-Js.

Section 1.0 Characterization of the Information

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

The application collects the bid preferences from the FSO along with supplementary statement that justifies why the FSO is the right choice for the position he or she is bidding for. Along with this information, the system also maintains the applicant's education, language scores, previous Washington DC and overseas assignments including assignments to hardship posts and citation and awards.

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

The applicant's profile data such as their education data, citation/awards data, previous overseas assignments and their language scores are being pulled in from iMART system. The applicant's bid preferences and supplementary statements are gathered from the applicants through application data entry screens.

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

The information collected by the system will be used by the FAS Program Area, Foreign Affairs (FA) Management Council to recommend job placements for the Foreign Service Officers to overseas posts.

1.4 How is the information collected?

Part of the information is obtained by reading posts and position related data from iMART system. The rest of the information is provided by the users of the system.

1.5 How will the information be checked for accuracy?

The supplementary data provided by the Foreign Service Officers is validated by FA. The accuracy of the remaining data is determined by iMART system and is also manually verified by FA.

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

Provisions for bidding are outlined in the contract with AFSA.

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

FSOBS collects the following: employee name, biographical information such as the bidder's current position and post, their foreign language scores, previous assignments, educational qualification and citation and awards. The system uses no employee or other information. 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. All FAS PII systems are encrypted at rest and in transit.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

The data collected through the application is used by Foreign Affairs management council to recommend placement of Foreign Service officers to vacant overseas posts.

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

The data collected through the application is used to generate various printable reports. The data is also used to populate form FAS-193 in PDF format and is used to create a Briefing Book used by the FA management council for their position assignment recommendations.

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

The system does not use publicly available data.

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

The application uses e-Authentication and role-based access to allow only authorized users. The user's data is further segregated, such that they will not be able to see each other's data.

Section 3.0 Retention

3.1 How long is information retained?

Records are maintained for a minimum of 1 year as defined by NARA records management policy. System backup and storage of the data is provided by DISC consistent with NARA and USDA policy for data retention.

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

FSOBS as child system of the MDA System, has undergone a Moderate level assessment and authorization process and consistent with FISMA, NIST, NARA, and USDA guidelines and has been authorized to operate at the Moderate system categorization level.

3.3 Privacy Impact Analysis: 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/FSOBS.

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 collected by the application is shared with FA Management Council. The shared information consists of the FSO bid preferences, supplementary statements from the FSOs, and actionable reports that the council could use to make placement recommendations.

4.2 How is the information transmitted or disclosed?

The information collected through the application is used to format and print form FAS 193 in pdf format. The printable forms are aggregated into a briefing book, along with other reports such as Post-Position assigned/unassigned user reports, bidding report by user etc,

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

Information sharing process is done outside the system, and Office of Foreign Affairs (FA) assumes the privacy risks associated with sharing of the information with FA management council.

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?

The data gathered through the application is not shared with any external organizations.

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.

Not Applicable. Data gathered is not shared with any external organizations.

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

Not Applicable

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

Not Applicable

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.

This system does not require a SORN

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

Before the start of the bidding cycle, FAS FA sends out a circular to the overseas posts informing the Foreign service employees about the upcoming bidding cycle.

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

The data solicited by the application is not mandatory, and is required only when the FSO's current assignment is coming to an end in the near future.

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

The application does not require the users to explicitly consent to data usage. The data collected by the application is used to decide the suitability of the candidate for assignment to vacant overseas posts.

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

The users of the application are fully aware of why the data is being collected. FA also sends out circular to overseas posts with detailed information about the upcoming bidding cycle.

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 have online access to their own data using their assigned control number and their registered eAuthentication account.

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

Upon detection of erroneous data in the employee profile, users would contact FAS HR with the correct information and HR would update the user profile in iMART system. The FSO Bidding system then periodically downloads the data from iMART system to overwrite any erroneous data with corrections.

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

Any errors in the user's profile data is caught by the users themselves. At that point they would work with the Agency HR outside the system and get the data corrected in iMART system. Those corrections would eventually flow into FSO Bidding system when it periodically pulls the data from iMART system.

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

The process is managed within FA.

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

With online access to their data and available privacy officer contact information there is minimal privacy risk regarding availability of redress.

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 training and signing specific rules of behavior.

8.2 Will Department contractors have access to the system?

Yes. They perform the application look up data maintenance and general administration activities. The access is limited to 1 or 2 contractors.

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

Users are provided annual security awareness training and users with specific security related positions are provided role based training.

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 boundary has been certified and accredited for operation including adequate security auditing procedures and technical safeguards to prevent misuse of data. Technically, FSOBS system is integrated with USDA e-Authentication software which requires all users of FSOBS to have an eAuthentication account. The technical safeguards are the application level and server level safeguard and security measures (Provided by D I S C). The application is protected with eauth and will not allow users to access without approval process.

8.6 Privacy Impact Analysis: 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 A&A process for MDA/FSOBS. The system does collect PII data and the primary privacy risks (undesired access) are mitigated by requiring eAuthentication 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?

FSO Bidding system is a web application implemented using Microsoft Dotnet framework, AngularJS and Microsoft SQL Server. The application uses USDA e-Authentication system to authenticate and authorize users. The system runs on hardware provided by DISC and runs on Microsoft Windows 2016 Operating system.

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

The system is not known to be using any technology that may raise privacy concerns

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?

This system does not use any third-party websites or applications.

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

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

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

N/A

If so, is it done automatically?

N/A

If so, is it done on a recurring basis?

N/A

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

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

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

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

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?

N/A

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A

10.12 Privacy Impact Analysis: 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

Responsible Officials

JONATHAN HEAL

Digitally signed by JONATHAN HEAL
Date: 2021.05.10 15:06:15 -04'00'

Jon Heal, MDA Project Manager
TFAA-FAS
United States Department of Agriculture

Approval

CAROL REMMERS

Digitally signed by CAROL REMMERS
Date: 2021.05.10 14:58:06 -04'00'

Carol Remmers
Privacy Officer
TFAA-FAS
United States Department of Agriculture