Privacy Impact Assessment for the International Activities and Financial Tracking System (IAFTS)

April 2023

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

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

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

Abstract

The Marketing Development and Administration's (MDA) International Activities and Financial Tracking System (IAFTS) is utilized primarily by the Office of Global Programs (GP) 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 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: FAS Cooperator data, company address, 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 FAS Cooperators and 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 Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

IAFTS does not collect public PII.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

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 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)?

Yes

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

All risk associated with data retention are addressed and have been mitigated in the System Security Plan and the Contingency Plan for the MDA/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 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 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 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 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 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?

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.

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 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.