Privacy Impact Assessment

for

FS Salesforce (FS SF)

Policy, E-Government and Fair Information Practices

Version: 1.1

Date: February 27,2020

Prepared for: USDA US Forest Service

Contact Point

Valdis Mezainis

System Owner

USDA NRE Forest Service

202-644-4621

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

This Privacy Impact Assessment (PIA) is for the United States Department of Agriculture (USDA) + FS Salesforce. FS Salesforce provides a USDA-wide system for processing, managing, and tracking business process affiliated with foreign visitors hosted in USDA facilities. This PIA is being conducted to determine the potential impact of the data which is collected via FS Salesforce.

Overview

USDA facilities host thousands of non-U.S. citizens each year for meetings, short term trainings, and long-term collaborative research projects. Each foreign visitor's information must be collected on a form (ARS-230) and logged into a "USDA Office of Homeland Security System" to initiate a name trace request prior to their expected arrival at USDA. The name trace process has multiple stakeholders and administrators across several USDA agencies and offices. An individual ARS-230 form will be handed off several times among stakeholders, whether for data input, approval, transfer to the "Homeland Security System", notification of clearance, and potential J-1 visa sponsorship action. As the document changes several hands, there are delays and errors and no visibility into any one individual request's progress in the process. In addition, the data collected is redundant as there are many other data collection systems used for other administrative process (visa sponsorship, applications for seminar or fellowship programs, etc.) involved in planning for and inviting a foreign visitor to be hosted in a USDA facility. Finally, there is a wide compliance gap with the name trace requirement across the range of USDA agencies that host foreign visitors (ARS, USFS, NRCS, FAS, APHIS, and GIPSA).

The project is designed to streamline and centralize data collection for foreign visitor "trips" to USDA facilities, provide a more secure method for treating the Personally identifiable information (PII) that is collected for the name trace process, reduce paperwork and errors, and provide transparency to all stakeholders into the progress of individual name trace requests. Improved processes and clear communication will lead to 100% compliance of name trace requirement. Beyond the pilot, full success will be reached when visitors are able to enter their own application and name trace data.

There are five modules that comprise the system:

Outreach Contact Module

Foreign Visitor Module

Detailer Module

Travel Module

Disaster Assistance Support Program Module

The Outreach Contact Module is the central set of data that the other modules of the program will connect to via the Contact ID number. This information is also used for collecting information from the Foreign Visitors, partners and parties interested in the services that is provided by the system. The system, using data from the Outreach Contact Module maintains contact to those that subscribe through service newsletters, and invitations to brown bags training seminars via email.

The Foreign Visitor Module collects information from people who are both interested in and have been accepted by the various hosts that the program interact with to work within the United States on different projects. This module helps International Programs service various agencies such as the Forest Service, Agriculture Research Service, and the Foreign Agriculture Service to track their visitors including host invitation, visa, financial obligations, fees, stipends, funding sponsorship, tax eligibility, and providing their information to the USDA Office of Homeland Security's name check program via email.

The Detailer Module is a database with in the system that gathers and tracks human resource information, acting as a knowledge base of skills within the Forest Service that could aid our various projects overseas.

The Travel Module collects the travel itineraries of various staff, contractors, and detailers who travel for International Programs. It will also allow the program to register for international SOS insurance for all program travelers.

The Disaster Assistance Support Program Module is the International Programs helps USAID Missions overseas with Disaster Mitigation Plans and various other forms of disaster management such as fires and floods. This module collects information on Forest Service Staff and various contractors with the requisite skill sets and experience to aid in these missions.

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 Identification

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

User level data is collected and tracked, necessary for provisioning foreign visitors host invitations, visas, debit card program, taxes, name and background checks, travel itineraries and other various programs.

User level data may include:

Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias

Date and/or place of birth.

Address Information (street or email address).

Personal identification number (e.g. passport number, driver's license number or a unique identification number, etc.)

Employment history.

Miscellaneous identification numbers (agency assigned number, case number, accounts, permits, contact id number, etc.)

Photographic image/identifying characteristics

Other (Copy of Passport)

1.2 Source

What is the source(s) of the information in the system?

The customer (foreign visitor) provides user level data, which contains PII, for provisioning and providing the FS Salesforce service.

1.3 Justification

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

FS Salesforce is designed to streamline and centralize data collection for foreign visitor “trips” to USDA facilities, provide a more secure method for treating the Personally identifiable information (PII) that is collected for the name trace process, reduce paperwork and errors, and provide transparency to all stakeholders into the progress of individual name trace requests. Improved processes and clear communication will lead to 100% compliance of name trace requirement.

1.4 Collection

How is the information collected?

The information is collected through online application (Salesforce) from which the customer (applicant) can input user level data and validate and edit their customer data. The USDA employees can review and process, manage, and track trace request.

1.5 Validation

Applications are checked for completeness based on requirements defined by FS Salesforce. Some completeness checks are automated and some are manually built into the workflow process. For example, there are required fields in the system where the permittee must enter data before proceeding to the next page of the application.

Manual verification involves the following steps:

The FS Salesforce reviewer confirms in FS Salesforce that all information was received and is complete.

If information is missing, they can use FS Salesforce to request more information as required.

1.6 Authority

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

The USDA Chief Information Officer (CIO) is responsible for developing and implementing security policies, programs, and standards to protect and safeguard the Department's personnel, property, facilities, and information. To do this, the OCIO has established access control policies designed to limit

access to USDA facilities to authorized individuals. In order to know if an individual is authorized access to a facility, the identity of the individual must be established. OCIO does this by obtaining PII related to the individual and then conducting appropriate checks of records maintained by FS Salesforce and other U.S. government agencies. Authorities associated with protecting federal property and information include:

5 U.S.C. § 301, "Government Organization and Employees;"

Section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. § 1441);

Executive Order 12977, "Interagency Security Committee;"

Executive Order 13286, "Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security;"

Presidential Decision Directive 12, "Security Awareness and Reporting of Foreign Contacts;"

Homeland Security Presidential Directive-7 (HSPD-7), "Critical Infrastructure Identification, Prioritization and Protection;"

National Infrastructure Protection Plan, "Government Facilities Sector," Sector-Specific Plan;"

Interagency Security Committee Standard, "Physical Security Criteria for Federal Facilities," April 12, 2010; and

Federal Property Regulations, July 2002.

1.7 Risk Mitigation

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

Risk: Ensuring the information the customer inputs into the system is accurate and up to date.

Mitigation: Authorized FS Salesforce personnel have knowledge of the user data that customers submit for FS Salesforce to provision and provide the service. FS Salesforce does not have visibility into the data stored by our customers within the service except for limited purposes specified in our customer contract. FS Salesforce encrypts the following fields as required: First Name, Last Name and employee ID. FS Salesforce relies on Salesforce for the implementation of all cryptographic mechanisms. Salesforce uses the

encryption methods described in the SSP for connection based encryption (firewall, Data, IPsec) and uses additional encryption methods (also defined in the SSP) for the custom fields in the application (letter, number, symbols) which meets FIPS 199 risk impact level for a Moderate system.

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 Usage

Describe all the uses of information.

The Outreach Contact Module is the central set of data that the other modules of the program will connect to via the Contact ID number. This information is also used for collecting information from the Foreign Visitors, partners and parties interested in the services that is provided by the system. The system, using data from the Outreach Contact Module maintains contact to those that subscribe through service newsletters, and invitations to brown bags training seminars via email.

The Foreign Visitor Module collects information from people who are both interested in and have been accepted by the various hosts that the program interact with to work within the United States on different projects. This module helps International Programs service various agencies such as the Forest Service, Agriculture Research Service, and the Foreign Agriculture Service to track their visitors including host invitation, visa, financial obligations, fees, stipends, funding sponsorship, tax eligibility, and providing their information to the USDA Office of Homeland Security's name check program.

The Detailer Module is a database with in the system that gathers and tracks human resource information, acting as a knowledge base of skills within the Forest Service that could aid our various projects overseas.

The Travel Module collects the travel itineraries of various staff, contractors, and detailers who travel for International Programs. It will also allow the program to register for international SOS insurance for all program travelers.

The Disaster Assistance Support Program Module is the International Programs helps USAID Missions overseas with Disaster Mitigation Plans and various other forms of disaster management such as fires and floods. This module collects information on Forest Service Staff and various contractors with the requisite skill sets and experience to aid in these missions.

2.2 Analysis and Production

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

N/A – no special tools are being used

2.3 Commercial/Public Use

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

No N/A – FS Salesforce does not use publicly available data

2.4 Risk Mitigation

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

N/A – FS Salesforce does not use publicly available data

Section 3.0 Retention

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

3.1 Time Period

How long is information retained?

All official Agency Records shall be retained and maintained as per NARA approved records retention schedules and per direction found in FSH 6209.11 (FS Records Management Handbook).

In the absence of an updated, approved Records Retention Schedule/Disposition Authority, all records are to be considered permanent and must be retained accordingly until otherwise/appropriately scheduled and approved by NARA.

In the absence of the agency policy for non-records the information will be retained for 5 years.

Where records are used as evidence in an investigation or in an administrative, litigation, or other proceeding, the records will be retained until final disposition of the investigation or proceeding.

3.2 Approval

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

Yes

3.3 Risk Mitigation

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

The retention period is in line with standard retention schedules for similar data and is long enough that any likelihood of having issues associated with the archiving or disposal of data is minimal.

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 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

FS Salesforce information is shared with the ARS Salesforce Portal as part of normal operations allowing applicants to input user level data, which contains PII, for provisioning and providing the FS Salesforce service. Salesforce uses the information to search its records for information about the subject.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

The information is shared through controlled user access as defined by system requirements. For example, based on a user's role, they may view a limited subset of information contained within the system based on their need for that data to perform their duties.

4.3 Risk Mitigation

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

FS Salesforce administration settings restrict access by requiring Admins and Content Custodians to invite authorized users to a folder or specific document. If the user has not been invited to collaborate by receiving a shared link they will not be able access content in FS Salesforce. It is possible to configure collaboration invites to allow users to view or submit content without allowing them to add other users or make changes. Collaborations permissions can be upgraded, downgraded, or removed entirely by users who have the rights to change the access control list.

Only Content Custodians (owners and co-owners) of the folder will be allowed to invite collaborators into a folder.

Overall the privacy risks are minimal as the system will be implemented in accordance to USDA & FS policies and guidelines. FS Salesforce's security

policies address the required security controls that must be followed in order to protect PII.

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 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

FS Salesforce does not share PII with external organizations.

5.2 Compatibility

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.

FS Salesforce does not share PII with external organizations.

5.3 Delivery and Security Measures

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

FS Salesforce does not share PII with external organizations.

5.4 Risk Mitigation

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

FS Salesforce does not share PII with external organizations.

Section 6.0 System of Records Notice (SORN)

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 Requirement and Identification

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

USDA/FS-19
DHS/ALL-039
OPM/GOVT-1
GSA/GOVT-4

6.2 Individual Notification

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

Prior to logging into FS Salesforce and providing information the user is required to acknowledge a privacy and security notice. This page also provides additional links that provides the user with direct links to the SORNs and further information on their rights.

6.3 Right to Decline

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

Individuals can decline to input their data into FS Salesforce, however their participation in a USDA program will be declined.

6.4 Right of Consent

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

The individual does not have the ability to consent of particular uses of the information collected in the system. If they acknowledge the collection of the information, they are providing the authorization to use the information for all purposes of reviewing, managing, tracking and issuing regulatory decisions regarding their sponsorship status. There is no ability to consent to individual uses of information. It is specifically called out that the individual agrees to the

use of this information by continuing past the screen describing the uses of their information.

6.5 Risk Mitigation

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

Individuals are provided sufficient notice as to their rights and are required to positively acknowledge receipt of this notice prior to using the FS Salesforce system. There is no way for a user to provide the information, without first acknowledging they understand the information is being collected and used for the purposes of reviewing, managing, tracking and issuing regulatory decisions regarding their sponsorship status.

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 Access

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

Individuals may review their information online at any time by viewing their submissions and responses.

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Prior to submission, users may self-correct any issues. After submission, Individuals may review their information online and edit their submission and responses. In some cases, the USDA may contact the user and request that they send additional information in order to correct deficient or erroneous information.

7.3 Notification

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

Wherever possible, the FS provides notice to individuals about its policies regarding the collection, use, and disclosure of information at the time the information is collected. The notice generally includes the procedures, or a reference, that individuals may use to correct their information. For information that is collected pursuant to a request from the FS, notice is generally provided as part of that request (e.g., in a letter request or in the document outlining the compulsory process request). The FS also provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one.

7.4 Redress Alternatives

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

Not applicable, a method of formal redress is available.

7.5 Risk Mitigation

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

Individuals are provided with the ability to review their information and any responses issued to them through the system at any time, and may contact the helpdesk to provide assistance with any issues they may have.

Section 8.0 Technical Access and Security

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

8.1 Procedures

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

FS Salesforce implements a Rules of Behavior (ROB) for which all users must consent prior to being granted systems credentials for access. The system inherits the USDA implementation of User Security Awareness training which is provided annually by the Department.

For the individuals using the public facing system FS Salesforce will implement the USDA internet use & copyright restrictions warning banner.

Content Custodian is defined as an individual (or individuals) who have responsibilities within a functional area for Forest Service information. They include unit line officers, file structure stewards, and/or content authors. For specific documents, they would be original creator or source for the information, and any other individual given the right/privilege to administer the data to include reading, sharing, deleting, and modifying. They are also defined as the persons who can select others with a need-to-know for read/view/modify of the PII data.

8.2 Contractor Access

Will Department contractors have access to the system?

Only specifically authorized Department contractors have access to the system. Those individuals must first obtain relevant security clearances along with specific authorization to access information at various levels.

8.3 Privacy Training

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

The system inherits the USDA implementation of User Security Awareness and Privacy training which is provided annually through AgLearn.

8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer “Yes” and provide ATO expiration date(s).

No

8.5 Audit and Technical Safeguards

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

All users are required to have an individual user account to the application system.

8.6 Risk Mitigation

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?

This information is protected through various levels of security and policy. The system itself is protected by role based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so.

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 Description

What type of project is the program or system?

Payroll and Benefits FS Salesforce is a web based application on a government cloud base system (Salesforce)

9.2 Privacy Concerns

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

The system does not utilize any technologies that would raise the Privacy Risk.

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 Review

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 Purpose

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

Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

10.4 PII Usage

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

Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

10.5 PII Maintenance and Security

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

Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

10.6 PII Purging

Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

N/ Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

10.7 PII Access

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

Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

10.8 PII Sharing

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?

Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

10.9 SORN Requirement

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)?

Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

No, FS Salesforce does not use web measurement and customization technology.

10.11 Web Measurement and Customization Opt-In/Opt-Out

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

No, FS Salesforce does not use web measurement and customization technology.

10.12 Risk Mitigation

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.

Not Applicable, FS Salesforce does not make use of 3d party websites or applications to process PII.

Responsible Official

VALDIS MEZAINIS
Digitally signed by VALDIS MEZAINIS
Date: 2020.05.06 16:50:59 -04'00'

Valdis Mezainis
System Owner (SO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS
Digitally signed by CYNTHIA TOWERS
Date: 2020.05.08 07:24:04 -05'00'

Cynthia Towers
Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

ROBERT CHADDERDON
Digitally signed by ROBERT CHADDERDON
Date: 2020.05.11 08:17:41 -06'00'

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture