Privacy Impact Assessment

FPAC Salesforce

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: August 12, 2021
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

FPAC Salesforce

August 12, 2021

Contact Point

Donald Simpson
FPAC Salesforce Information System Owner
FPAC BC
(202) 260-9247

Ravikanth Kondapalli
FPAC Salesforce Program Manager
FPAC BC
(816) 926-3012

Reviewing Official

James Flickinger
FPAC Assistant Chief Information Security Officer
United States Department of Agriculture
(816) 926-6010

Abstract

FPAC Salesforce is a platform owned by Salesforce GovCloud that hosts several FPAC applications; some of these applications contain PII.

A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law 107-347, 44 U.S.C. §101).

Overview

FPAC Salesforce is the combination of these NRCS and FSA applications:

1. **The FPAC/NRCS Business Operations Tool (BOT)** will automate the basic functions of business operations management needed to support the day-to-day procurement activities. It includes managing the NRCS Office of the Chief Information Officer (OCIO) "Checkbook", developing cost models, recording and storing all Information Technology (IT) contracts and agreements, and supporting the AD-700 procurement process
2. **The FPAC/NRCS Regional Conservation Partnership Program (RCPP)** encourages partners to join in efforts with producers to increase the restoration and sustainable use of soil, water, wildlife and related natural resources on regional or watershed scales. Through the program, NRCS and its partners help producers install and maintain conservation activities in selected project areas. Partners leverage RCPP funding in project areas and report on the benefits achieved.

   Partners also use the RCPP application to submit proposals containing the following information which is stored in the system for further processing:

   • Project Information (e.g. Name of the project, Location, purpose, etc.)
   • Partners Information (e.g. Names, Addresses, Email, Phone Number, DUNS ID, etc.)
   • Financial Information

   The RCPP application does not share any information with any external system. Only authorized users will be able to access the important information once their accounts are authenticated via e-Auth.

3. **The FPAC/NRCS CSP Application Evaluation Tool (CAET)** will allow field users to evaluate the applicant's existing conservation activities. CAET will not be accessed by any external users. All access will be by USDA National, State, and Field office users utilizing their eAuth Level 2 accounts. These users will manually input applicant (farmer/producer) information such as their name, state of residence, county of residence, ProTracts contract number, ranking pool (socio/economic factor), and field office name into the CAET for eligibility determination. A PDF report is then

generated from CAET and used to manually input all farmer information into the separately accredited ProTracts-FundManager (PT-FM) system.

4. **The FPAC/NRCS Technical Service Provider (TSP) Registry** is the central system for Technical Service Providers (TSPs). TSPs can manage their profiles and certifications. Businesses can manage their profiles and associate with TSPs. NRCS staff can review applications, certify TSPs, and audit TSPs after certification. There is also a public-facing portal where clients can search for certified TSPs and businesses to hire to complete work.

5. **The FPAC/FSA Portal (FPAC-P)** creates a singular and intuitive user experience for both the American Producer and the USDA personnel that support the FPAC mission through this system.
   - Ability to provide a "My Documents" view for both a Producer (Farmer/Rancher) and a USDA Employee looking on behalf of a Producer – where the user can see all documents and open documents (based on allowable permissions)
   - Ability to take appropriate actions on a "My Documents" document such as edit, sign, etc.
   - Ability to download relevant forms
   - Ability to sign and scan forms to upload manually to a folder both for Producer and USDA employee on behalf of (for example, sign, scan and upload a direct deposit form)
   - Ability to design a completed form online
   - Upon document upload, ability to trigger notifications to designated service center
   - Ability to see pending requests related to a document (i.e. pending signature request) and to allow authorized producer or designee to perform the e-signature
   - Ability to provide a "My Applications" list view of all applications with key metadata shown
   - Ability to manage applications from a summary view and take any of the following actions such as Create/Edit Agreements, Request Agreement Modification, View Agreement Details, Sign an Agreement (electronic and/or manual), etc.
   - Ability to provide a list view of "Manage Plans and Practices" documents and "Manage Plan Details" for Plan Documents. Provide views of metadata around Plan Details.
   - Ability to import documents of various file types and associate them with Producer records and to also view such records.

   To perform these activities for FPAC-P, this information is collected from customers: Name, email address, date of birth, personal identification number (SSN), financial data, core customer ID.

   FPAC-P uses the following components:

   5.1 Component of FPAC/FSA's FPAC-P: Bridges to Opportunity (BTO) is a portal for customers, partners and resource managers to list and search for information

on opportunities provided agricultural stakeholders. The BTO application has supplementary add-on products which support of the main function.

- **Coveo** is a separate application which provides the main search functionality for the customer interactions in BTO. The data indexed within the Coveo application includes BTO content and information from external websites.
- **Timba Surveys** is an add-on module provided by SalesForce and supports the customer feedback process, where information is collected on the customer experience and reviewed to improve the business process. Survey information is collected anonymously from external customers or they have the option of populating this information electronically.
- **Knowledge** is used to create a fully functional information repository where users can search, store, and send information to both internal stakeholders and external customers.
- **CRM Content** is a built-in feature that allows users to upload files and share them to external users.

5.2 Component of FPAC/FSA's FPAC-P: Wildfires & Hurricanes Indemnity Program (WHIP) controller with users assigned National/State Office Information Profile (OIP) code allows select employees to view/create/edit & approve/disapprove applications. National users can delete/archive apps, configure labels, lists, etc.

Legal Authority: This system is regulated by privacy laws, regulations and government requirements, including the Clinger-Cohen Act of 1996; the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101); the Paperwork Reduction Act of 1995 (44 U.S.C. §3501). Guidance can be found in Appendix III to OMB Circular A-130 and NIST SP-800-30, Risk Management Guide for Information Technology Systems.

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?

- BOT does not create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII
- RCPP Partner Portal collects and maintains partner information (containing PII) and project proposal data (containing PII) from NRCS partners. For instance - Name of the project, Location, purpose, Partner Names, Addresses, Email, Phone Number, DUNS ID, etc.

- CAET collects and maintains the name of the applicant, Protract Contract Number, and the Name of the state/Field office of the applicant.
- More information on the information collected can be found here: http://www.grants.gov/view-opportunity.html?oppId=291192
- TSP Registry collects contact information such as address, phone, and email as well as profile information such as education, work experience, and licenses/certifications.
- FPAC-P collects Customer name, email address, date of birth, personal identification number (SSN), financial data – assets, liabilities, equity, income, expenses, and cash flow, core customer ID – unique identification number used to identify ranchers, farmers and producers, similar to an account number used by a local utility company.

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

- RCPP collects information directly from NRCS partners through the RCPP Application – pre-proposal and full-proposal. CAET collects information from CAET participants, also known as farmers and producers. TSP Registry information is entered by the TSPs.
- FPAC-P obtains information from Farm Service Agency (FSA), ongoing data is entered by authorized USDA Service Center employees

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

- RCPP Partner Portal is a voluntary conservation program that encourages organizations to partner with NRCS to address resource concerns across the nation. Information is necessary to assess eligibility and also evaluate the partnership proposals.
- CAET is a voluntary conservation program that encourages producers to address resource concerns in a comprehensive manner by undertaking additional conservation activities; and improving, maintaining, and managing existing conservation activities.
• TSP Registry information is necessary to evaluate the user for becoming a certified TSP.

1.4 How is the information collected?

- Data is collected from customers and employees and entered into the FPAC-P by FSA and county office employees
- RCPP information is collected directly from NRCS partners, and not from any third-party sources.
- CAET information is not collected directly from the applicant, but information is inputted by NRCS employees.
- TSP Registry information is entered directly by the TSP. PII data is not collected by any third-party sources.

1.5 How will the information be checked for accuracy?

- For FPAC-P, data collected from the customer is required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.
- NRCS employees review applications and proposal submissions. In addition, application logic checks are in place.

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

- For FPAC-P, Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397, the Agricultural Act of 2014 (Pub. L. 113-79), the Agricultural Improvement Act of 2018 (Pub. L. 115-334), and the Coronavirus Aid, Relief, and Economic Security Act (CARES ACT) (Pub. L. 116-136)
- USDA RCPP Program (http://www.grants.gov/view-opportunity.html?oppId=291192)
- The Regional Conservation Partnership Program (RCPP) is authorized by Subtitle I of Title XII of the Food Security Act of 1985 (the 1985 Act), as amended by Section 2401 of the Agricultural Act of 2014 (the 2014 Act). The Secretary of Agriculture has delegated the authority to administer RCPP to the Chief of the Natural Resources Conservation Service (NRCS), who is Vice President of the Commodity Credit Corporation (CCC). NRCS is an agency of the Department of Agriculture (USDA).
- USDA CAET program
- USDA TSP Program: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/programs/technical/tsp/

- These regulations pertain: • Privacy Act (5 U.S.C. 552a);
- E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101);
- Paperwork Reduction Act of 1995 (44 U.S.C. § 3501)

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

- Privacy risk are minimal as privacy information is inputted only by partners and NRCS government employees that have access to the application. Under our current plan, users must be authenticated via USDA ICAMs e-AUTH system and authorized via USDA's role-based authorization
- The privacy risks are moderate. The minimum amount of personally identifiable information is collected to satisfy the purpose of this system. The risks are mitigated using various control mechanisms, these include:
- All users must be uniquely identified and authenticated prior to accessing the application.
- Access to data is restricted.
- Information is encrypted at rest and in transit.
- Masking of PII

- System audit logs are retained and reviewed weekly

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.

- For FPAC P, "one-stop shops" for farmers seeking information and opportunities to a broader array of services provided by county, state and national agricultural stakeholders. This includes:
  - Name (full name, mother's maiden name, maiden name of individual, nickname, or alias
  - Date and/or place of birth
  - Address information (street or email address)
  - Personal identification number (e.g. social security number, tax identification number, passport number, driver's license number or a unique identification number, etc.
  - Miscellaneous identification number (agency assigned number, case number, accounts, permits, etc.)
  - Other information that may be seen as personal (personal characteristics, etc.)
- RCPP Partner Portal is a voluntary conservation program that encourages organizations to partner with NRCS to address resource concerns across the nation. Information is necessary to access partnership proposals. This includes:
  - Core Customer ID
  - Proposal/Project numbers
  - DUNS numbers
  - Personal information collected in FPAC-P above
- CAET is a voluntary conservation program that encourages producers to address resource concerns in a comprehensive manner by undertaking additional conservation activities; and improving, maintaining, and managing existing conservation activities.
- TSP Program is a voluntary program that allows individuals to become certified in specific practices in order to get and perform certain types of work. Information is necessary to evaluate applicant for certification and to provide technical services to farmers and ranchers on behalf of the USDA. This includes the personal information collected in FPAC-P above.

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

- RCPP Partner Portal uses standard Salesforce reporting to analyze data. CAET will analyze the data and ascertain eligibility. TSP Registry uses standard Salesforce reporting to analyze data.

- No Other tools are used to analyze the data

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

- CAET collects commercial or publicly available data from CAET participants on their conservation practices.
- No other commercial or public 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.

- Access to the system and data are determined by business need and individual roles. Controls are in place to provide reasonable assurance that data integrity and confidentiality are maintained during processing. Controls in place to ensure the correct handling of information include the following:
- End users are correctly identified and authenticated according USDA and FSA security policies for access managements, authentication and identification controls.
- Audit logging is performed at the Department-level to ensure data integrity.
- This application is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.
- If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes

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?

- FPAC-P retains the information indefinitely (permanent records).
- Partner, proposal and TSP information is retained while the application remains in production.
- Per the NRCS System of Record Notice (SORN), “Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs”. Thus, any PII information that is retained will be retained for sufficient periods of time (approximately 10 years) to ensure compliance with the Farm Bill and any other applicable legislation and regulations. USDA/NRCS-1: Landowner, Operator, Producer, Cooperator, or Participant Files

- CAET information is retained for a period no longer than 5 years. This is the NRCS policy and limits the payment period for any approved conservation practice for up to 5 years.

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

- Yes, in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records.

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

For FPAC-P:

- During this period, the stored information may be at risk for viewing by unauthorized parties, data loss or destruction and non-availability. Access to computerized files are protected by access control software, physical access controls and if warranted, password-protected.
- SORN USDA/FSA-2 States: Program documents are destroyed within 6 years after end of participation.
- According to Records Management DR3080-001 Disposition of Inactive Records: Records and other documents that are no longer sufficiently active to warrant retention in office space shall be removed as rapidly as possible by: (a) transfer to a Federal Records Center, or (b) transfer to a records retention facility meeting the requirements of 36 CFR Chapter 12, Subchapter B Records Management, Subpart K, 1228.224 through 1228.244, or (c) if authorized, by disposal
-

For other data on the system:

- Privacy risk for breach of data that could result inappropriate use or exposure is mitigated through appropriate access control, controlled approved facilities for the system, and appropriate handling procedures.
- The primary privacy risk is that a data breach could result in the release of information on members of the public. This is mitigated by limited access to the data, non-portability of the data and controlled storage of the data in controlled facilities.
- Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed above.

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 collected information (including PII) by RCPP is shared with the NRCS/USDA Grants & Agreements, contracts, and financial payment programs. Information is used to assess project proposals.
- CAET collected information is shared with the NRCS/USDA financial payment programs and Protracts.
- TSP contact information such as address, phone, and email as well as profile information such as education, work experience, and licenses/certifications are shared with NRCS employees working with the TSP Registry.
- FPAC-P does not share data.

4.2 How is the information transmitted or disclosed?

- Internal organizations will access RCPP information through the RCPP portal and will be able to generate a PDF. CAET information is transmitted through a PDF that is uploaded manually to other NRCS systems through an out of band manual process.
- TSP information is accessed through the TSP Registry application via eAuth level 2 authentication.
- FPAC-P does not transmit or disclose data.

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.

- For the applications that share or disclose data, privacy risks are mitigated as PII information is minimal and is only accessed and handled by NRCS-authorized roles and e-authenticated personnel.
- Privacy risks are mitigated by ensuring that access to the data is through established security rules via eAuth. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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?

- For RCPP only, partner names and addresses are shared with other partner organizations to provide contact information necessary for partners to make partnerships with each other.
- TSPs can choose to share their profile on the public-facing portal so clients can search for them and hire them to complete work. Certain information such as license numbers is withheld from the public-facing portal.
- No FPAC-P application information is being shared outside of the USDA environment.

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.

- RCPP and CAET - Information may be shared with other partners and would be used to contact the lead partners regarding partnership opportunities.
- TSP Registry – Limited information shared externally (i.e., Name, address, phone number). Shared information covered under SORN NRCS-1.
- No FPAC-P application information is being shared

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

- Information is shared via the RCPP. Externally shared information and security measures are covered under SORN USDA/NRCS-1
- TSP Registry information is shown on the public-facing portal via Salesforce pages. There is a Salesforce profile for public users that restricts access to data just like any other user.
- No FPAC-P application information is being share

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

- Privacy risks are mitigated as PII information is minimal and is only accessed and handled by NRCS-authorized roles and e-authenticated personnel.
- TSP Registry - access is restricted by Salesforce profiles. Information is also voluntarily shared by the user.
- No FPAC-P application information is being shared

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.

- NRCS Records are subject to USDA/NRCS-1

- FSA Records are subject to USDA/FSA–2 - Farm Records File (Automated) and USDA/FSA-14 - Applicant/Borrower.

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

- Yes:
  - under mandatory RCPP and CAET program guidelines. The below link to the NRCS Privacy Policy is placed on the application Please see: https://www.nrcs.usda.gov/wps/portal/nrcs/detailfull/national/about/?cid=nrcsdev11_000885 under NRCS Registry guidelines. The information is inputted by the user voluntarily.
  - NRCS Privacy Policy published on USDA website.

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

- Yes, under mandatory RCPP and CAET program guidelines. The below link is placed on the application Please see: https://www.nrcs.usda.gov/wps/portal/nrcs/detailfull/national/about/?cid=nrcsdev11_000885.
- Yes, under TSP Registry guidelines. The information is inputted by the user voluntarily. TSP Registry is a voluntary program.

- Yes for FPAC-P. FSA Privacy Policy refers individuals to the USDA Privacy Policy. Please see: https://www.fsa.usda.gov/help/privacy-policy/index

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

- Yes, under mandatory RCPP program guidelines. The below link is placed on the application Please see: https://www.nrcs.usda.gov/wps/portal/nrcs/detailfull/national/about/?cid=nrcsdev11_000885
- Yes, under TSP Registry guidelines. The information is inputted by the user voluntarily.
- Yes, for FPAC-P, in accordance with FSA Privacy policy and the individual's written consent. Please see: https://www.fsa.usda.gov/help/privacy-policy/index

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.

- Prior to accessing any system of record. All users are provided a notice prior to logging in via eAuth.
- Privacy risks are mitigated as links are provided on the application to the NRCS Privacy Notice, which provides all rights PII information is minimal and is only accessed and handled by NRCS-authorized roles and e-authenticated personnel.
- NRCS agents also provide manual notices under the mandatory RCPP and CAET program guidelines.
- Privacy risks for NRCS Registry are mitigated as all information is inputted by the user voluntarily.
- For FPAC-P: The risk is considered moderate. Notification is automatically provided in the system of records notice (Federal Register publication): SORN: USDA/FSA–2 - Farm Records File (Automated) and USDA/FSA-14 - Applicant/Borrower.

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?

For NRCS Applications:

- Access is gained through USDA's e-authentication and role-based authorization. See the link under 6.1.
- Users of NRCS Registry have access to view/edit all information they input at any time and access is gained through USDA's e-authentication level 2 and role-based authorization.
- Partners request access through the RCPP Program Team, who then registers the partners within the portal if they are approved.
- As published in SORN USDA/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

For FPAC-P:

- As published in SORN USDA/FSA-2 and SORN USDA/FSA-14: "An individual may obtain information about a record in the system which pertains to such individual by submitting a written request to the above listed System Manager. The envelope and letter should be marked "Privacy Act Request." A request for information should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

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

For NRCS Applications:

- NRCS agents follow redress and correction procedures under the mandatory RCPP program guidelines. See the link under 6.1.
- Partners are able to directly correct inaccuracies/errors in their name and/or addresses by working with the RCPP Team.
- CAET privacy risks are minimal as mitigation procedure include the application does not collect PII from any individual. NRCS agents follow redress and correction procedures under the mandatory CAET program guidelines.
- NRCS Registry users have access to view/edit all information they input at any time.
- As published in SORN USDA/NRCS-1: "Any individual may obtain information as to the procedures for contesting a record in the system which pertains to him/her by submitting a written request to the district conservationist or his/her designated representative or to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013."

For FPAC-P:

- As published in SORN USDA/FSA-2 and SORN USDA/FSA-14: "Individuals desiring to contest or amend information maintained in the system should direct their request to the above listed System Manager and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information to help identify the file."

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

- NRCS agents follow redress and correction procedures under the mandatory RCPP program guidelines. See the link under 6.1.
- Partners are able to directly correct inaccuracies/errors in their name and/or addresses by working with the RCPP Team.

- Information inputted into CAET is governed under overarching USDA CAET program guidelines.
- NRCS Registry users have access to view/edit all information they input at any time.
- Formal redress is provided via the FSA Privacy Act Operations Handbook. 03-INFO_R00_A04, Privacy Act Operations (usda.gov)
- The USDA SORNs are published on the USDA OCIO System of Records website. https://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records

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

- NRCS agents follow redress and correction procedures under the mandatory RCPP program guidelines. See the link under 6.1.
- Partners are able to directly correct inaccuracies/errors in their name and/or addresses by working with the RCPP Team.
- Information inputted into CAET is governed under overarching USDA CAET program guidelines.
- NRCS Registry users have access to view/edit all information they input at any time.
- Does not apply to FPAC-P as formal redress is available
- As published in SORN USDA/NRCS-1: "Any individual may obtain information as to the procedures for contesting a record in the system which pertains to him/her by submitting a written request to the district conservationist or his/her designated representative or to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013."

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

- Privacy Act Concerns involve an individual's rights to correct or redress their information that is held by the agency. These concerns are mitigated as NRCS agents follow redress and correction procedures under the mandatory RCPP program guidelines.
- PII information is minimal and is only accessed and handled by NRCS-authorized roles and e-authenticated personnel.
- CAET privacy risks are minimal as mitigation procedure include the application does not collect PII from any individual. NRCS agents follow redress and correction procedures under the mandatory CAET program guidelines.
- Privacy risks for NRCS Registry are minimal as users have access to view/edit all information they input at any time.
- For FPAC-P, the risk associated with redress is considered low, as the public does not have access to the system or the data. While the public cannot access the system to update

or change their personal information, they may update their information using form AD 2530 and submit to the appropriate FSA official. The FSA official will in turn update the system based on the information provided.

- Any PII information obtained from the SCIMS SharePoint site would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to correct their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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?

- Access to NRCS applications are determined via a valid e-Auth ID and password (level 2) on a valid "need to know" basis as determined by requirements to perform applicable official duties. For internal users, level of access is determined by zRoles (RBAC).
- The application has documented Access Control Procedures, in compliance with FISMA and USDA directives.
- For FPAC-P, FSA-13-A is used to request user access to USDA and FSA information technology systems including specifying authorization for accessing the system. (Refer to Notice IRM-440 - https://www.fsa.usda.gov/Internet/FSA_Notice/irm_440.pdf) In addition, access to FSA web applications is gained via an on-line registration process similar to using the FSA-13- A form.

8.2 Will Department contractors have access to the system?

- Yes, Department contractors with a need to know will have access to RCPP as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements and must obtain Level 2 eAuthentication access
- As part of the FPAC onboarding process, contractors must meet all requirements for access to applications. Through the USDA Rules of Behavior, they are not allowed to download, share, store or print any USDA specific data.
- All roles are approved on a need-to-know basis via FPAC BC management
- Contractors are required to sign NDAs as per the USDA FPAC BC Onboarding process
- Department contractors do not have access to any other FPAC Salesforce applications.

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

- NRCS requires that every employee and contractor receive Information Security Awareness training before being granted network and account access, per General Manual, Title 270, Part 409 – Logical Access Control and Account Management.
- Annual Security Awareness and Specialized Training, and Privacy training, is also required, per FISMA and USDA policy, and is tracked by USDA.
- For FPAC-P, once hired, Information Security Awareness Training and Rules of Behavior training is completed prior to gaining access to a workstation. The privacy training addresses user's responsibilities to protect privacy data and how to protect it.

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

- FPAC Salesforce is a Moderate system
- The most recent ATO renewal for FPAC Salesforce was September 4, 2020. Expiring September 4, 2023
- Previously, FPAC Salesforce was the combination of two systems, both had existing ATOs.

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

- NRCS complies with the "Federal Information Security Modernization Act of 2014" (FISMA). Assessment and Accreditation, as well as annual key control self-assessments, and continuous monitoring procedures are implemented for this application per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 4.
- NRCS complies with the specific requirements for "auditing measures and technical safeguards" that are provided in OMB M-07-16, including the security requirement that all data on mobile computers/devices containing agency data must be encrypted using only NIST certified cryptographic modules.
- Encryption that is performed outside of the accreditation boundary of this application is discussed in Section 8.6 below. Given the limited sensitivity and scope of the information retained, this application does not encrypt PII within the database.
- Masking of applicable information is performed outside of the accreditation boundary of this application (e.g., passwords are masked by e-Auth). This application does not process the type of very sensitive PII that would require masking (e.g., SSN). Given the limited sensitivity and scope of the information retained, this application does not mask PII (e.g., "Name" is not masked).
- Controlled access to PII is implemented outside the accreditation boundary of this application (e.g., via multi-factor authentication for remote access). While the PII

information retained has limited sensitivity and scope (i.e., the Name of non-employee "affiliates"), this application does control (limit) access to PII. The access of an Affiliate user (i.e., an NRCS employee) is generally limited to the "scope" of their office.

- Timeout for remote access is implemented outside of the accreditation boundary of this application (e.g., by e-Auth), so this application does not need to implement timeout for remote access to PII due to inactivity.
- System audit logs are implemented outside of the accreditation boundary of this application. This includes internal audit logs that are used to ensure that administrative functions and activities are being logged and monitored (e.g., modifications, additions, and deletions of privileged accounts per the e-Authentication SLA). Given the limited sensitivity and scope of the information retained, this application does not implement system audit logs related to PII integrity, nor does this application implement a Security Information and Event Management (SIEM) log management system. No auditing, e-Auth controls everything.
- For FPAC-P, the logging/auditing mechanism is an inherited function. The Application does not generate its own log/audit information. Any logging and auditing of access, transactions or output is left to the OCIO-ITS, and eAuthentication Application.

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 concern involving collection information is mitigated by the use of encryption, controlled access, and system audits.
- Privacy risks are mitigated as PII information is minimal and is only accessed and handled by NRCS-authorized roles and e-authenticated personnel.
- Data extracts containing PII are not regularly obtained from the system, therefore, privacy risk from this area is limited and addressed through IT Data Extract processes controls.
- For FPAC-P, the main risk associated with privacy is the exposure to unauthorized access to privacy information. This risk is considered moderate. Mitigating controls are in place to ensure privacy risks are minimal. Mitigated controls are mapped back to SSP in CSAM.
- Quarterly access reviews are done to ensure controls are mitigated.

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?

- FPAC Salesforce applications reside on the USDA Salesforce GovCloud Platform.

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

- Privacy concerns are mitigated based on security safeguards elaborated in the Salesforce's FedRAMP Authority to Operate (ATO) and USDA Salesforce ATO for cloud systems.

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"?

- N/A, 3rd party websites are not used.

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

- N/A, 3rd party websites are not used.

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

- N/A, 3rd party websites are not used.

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, 3rd party websites are not used.

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, 3rd party websites are not used.

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

- N/A, 3rd party websites are not used.

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, 3rd party websites are not used.

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, 3rd party websites are not used.

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, 3rd party websites are not used.

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?

- N/A, web measurement and customization technology are not used.

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.

- Risks are nominal as the websites are owned and controlled by NRCS personnel and no third party companies or organizations have access.
- Risk concerns are mitigated as USDA has procured licenses for building the application on Salesforce's Government Cloud platform. The application built on Salesforce is owned by USDA. Salesforce GovCloud holds a FedRAMP attestation and the USDA ASOC has also issued an ATO for the Salesforce platform.

Agency Responsible Officials

DONALD SIMPSON

Digitally signed by DONALD SIMPSON
Date: 2021.09.21 15:44:02 -04'00'

Donald Simpson
FPAC Salesforce Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS

Digitally signed by LANITA THOMAS
Date: 2021.09.21 15:56:30 -04'00'

Lanita Thomas
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2021.09.21 08:07:21 -05'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture