Privacy Impact Assessment

ProTracts-FundManager

Policy, E-Government and Fair Information Practices

- Version: 3.1
- Date: February 17, 2021
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department
of Agriculture

Privacy Impact Assessment for the ProTracts-FundManager

February 17, 2021

Contact Point

Anthony Whitt
Project Manager, FPAC-BC
(970) 825-9796

Reviewing Official

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

Abstract

The Farm Security and Rural Investment Act of 2002 (Farm Bill) provides for technical and financial assistance to agricultural producers to conserve resources, maintain and improve the environmental health and productive capacity of their land. The Farm Bill gave NRCS responsibility for several conservation programs: the Environmental Quality Incentives Program (EQIP), the Wildlife Habitat Incentives Program (WHIP), the Agricultural Management Assistance Program (AMA), the Conservation Security Program (CSP), the Wetlands Reserve Program (WRP), and the Grasslands Reserve Program (GRP). The Program Contracts System, known as ProTracts/FundManager, application is a vital tool utilized to facilitate these responsibilities.

Overview

ProTracts-FundManager is a system of the Natural Resources Conservation Service (NRCS). NRCS provides private landowners with advice, guidance and technical services to carry out conservation practices. The NRCS is an agency within the USDA that has provided over 75 years of leadership in a partnership effort to help America's private landowners and managers. NRCS works with its partners to conserve their soil, water, and other natural resources by providing financial and technical assistance based on sound science and technology suited to a customer's specific needs.

The purpose of PT-FM is to manage NRCS conservation program applications, cost share contracts, and program fund management. PT-FM is used to manage funds allocated from the Financial Management Modernization Initiative (FMMI) system to state controlled sub accounts, it allows tracking those funds, and managing the applications and contracts associated with those funds. Authorized program payments are generated by electronic fund transfer from FMMI. Internal controls prevent over-obligation of program funds when applications are selected for funding, contracts are signed and obligated, payments are approved and contracts are modified.

Pro-Tracts is used to manage conservation contracting activities from application through contract completion. The functions include application tracking, production of filled application and contract forms, and access to automatic generation of applicant letters, practice certification, payment approval and filled payment application forms.

There is the ability to generate reports that are used for program management purposes. Output from PT-FM is in the form of hardcopy paper forms, lists, reports, and contracts. PT-FM provides several methods to generate reports or lists that can be printed or exported to Microsoft Excel.

Note: PT-FM does not process any financial transactions.

PT-FM links to several NRCS and USDA systems:

- The *Performance Results System (PRS)*, the NRCS system that tracks the impact of conservation practices on selected natural resources. This link allows field conservationists to certify practices for completion in PT-FM and report the completed practice in PRS with having to re-enter the information.

- The *Office Information Profile* (OIP), the database of USDA service center agency offices. This link provides an efficient enrollment process for PT-FM users.
- The NRCS *SmarTech Conservation Practice Physical Effects and Practice Average Costs* modules which are the repository of natural resource data and cost data that link to program ranking tools in ProTracts.
- PT-FM is indirectly linked to FMMI through the Fund Manager. FMMI is the USDA accounting system that tracks program allocations, obligations, and electronic fund transfer. Transactions such as payment approvals are initiated in PT-FM and transmitted to Fund Manager. Fund Manager transmits transactions to FMMI in the required format.
- PT-FM provides a sophisticated infrastructure that allows state program managers to configure permissions to match their state’s program management procedures. Because individual states have the authority to manage conservation programs according to local needs, the software had to be configurable to be accepted by state program managers.
- The *Conservation Measurement Tool (CMT)* evaluates *Conservation Stewardship Program (CSP)* applications using a point-based system to measure a relative environmental benefit. The tool evaluates existing and proposed new activities to calculate conservation performance points that will be used for ranking and payment purposes. Each operation is evaluated based on the operation’s merits. The CMT is size neutral, which means that similar operations (despite the size of each operation) have the same potential to accrue a similar number of points.

Legal Authority: This system is regulated by privacy laws, regulations and government requirements, including the Privacy Act (5 U.S.C. §552a); 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); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559); OMB Memos M-03-22, M-10-22, M-10-23, M-16-24, and M-17-12; and OMB Circular A-130, Appendix I.

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?

- PT-FM receives PII from the SCIMS database copy (see Section 1.2). The PII that is used and maintained by PT-FM includes the names, address, SSN/TIN, and bank account information of members of the public, program participants, farmers, ranchers, and producers.
- PT-FM uses and maintains information acquired from the SCIMS database copy to identify program participants and information to ensure that appropriate payments can be made.
- As reflected on the FSA PIA for Customer Name/Address Systems (CN/AS) Service Center Information Management System (SCIMS), in response to 1.1, the following information is collected, used, disseminated, or maintained:
  - Customer: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation. Name & Address (MF) includes Farm Service Agency employees, farm owners, farm operators, and Technical Service Providers. Additionally business customers can be identified by business entity type (i.e. general partnership, Limited Liability Company, corporation, etc.)
  - Employee: Name, gender, citizenship country, address, race, veteran status, receive mail option, limited resource producer status, resident alien status, birth date, marital status, voting district, language preference, ethnicity, disability information, and other basic information such as Social Security Number, Employer Identification Number, mailing address, email address, phone numbers and Program Participation

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

- The *Service Center Information Management System* (SCIMS), maintained by FSA, Service Center Information Management System (SCIMS), CSAM ID # 1672, is the database of customer information that is shared by the three Service Center Agencies, FSA, NRCS, and Rural Development. SCIMS is a repository for USDA business entity and conservation compliance information. This link allows the most current customer

information to be printed on forms and letters. It also allows NRCS managers to generate reports on the race, sex, national origin, and disability of program applicants and participants.
- NRCS has access to a copy of the SCIMS database via replication and access to the data from SCIMS for NRCS users is via NPAD and through eAuthentication (eAuth). NRCS users do not have direct access to SCIMS. The landowners and general public applicants may provide information to SCIMS, which is the source of the PII. All information is obtained through a database copy. PT-FM does not modify or update any information in SCIMS.

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

- PT-FM does not directly "collect" any PII from any affected individual.
- PT-FM uses and maintains the PII information obtained from the SCIMS database copy to assist NRCS program participants in managing conservation contracting activities from application through contract completion. Legislation mandates participants and their land meet certain eligibility requirements.

1.4 How is the information collected?

- PT-FM does not directly collect any PII from affected individuals (i.e., members of the Public, program participants, farmers, ranchers, producers), nor is PII collected from any other third-party sources, other than the SCIMS system.
- PT-FM collects landowner information, including the names, addresses, SSN/TIN, and bank account information, using the SCIMS ID of the affected individual and SCIMS IDs from the SCIMS database copy. NRCS users do not have a direct access to SCIMS. All information is obtained through a database copy.

1.5 How will the information be checked for accuracy?

- Information in PT-FM is reviewed for accuracy and is verified through manual review and comparison with existing agency data. This is done by NRCS personnel who have the requisite knowledge and responsibility for the data.
- The accuracy of PII obtained from SCIMS or other applications not maintained by NRCS is not within the scope of PT-FM. PT-FM does not have the ability to update any information in SCIMS, nor does it have the ability to update the information in any other application databases not maintained by NRCS.

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

These regulations are applicable:
- 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.

- PT-FM does not directly "collect" any PII from any affected individual (i.e., member of the public).
- PII information is obtained from SCIMS and other documents, as discussed in the PIA Overview and Section 1.1.
- Privacy risks are mitigated as access to the information will be limited because users are authenticated by eAuthentication, and once authenticated, the user is directed to the application URL. Access to the website is through a load share switch to one of three Web Servers. PT-FM utilizes a Role Based Access Control (RBAC) model for end-user access to the application.
- Please see Section 2.4 and Section 8.6 for a further discussion of security controls that are in place to mitigate privacy risks.

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 A&A (and PIA) purposes, ProTracts and FundManager are considered as one application.
  - ProTracts is used to manage conservation contracting activities from application through contract completion. The functions include application tracking, production of filled application and contract forms, and access to automatic generation of applicant letters, practice certification, payment approval and filled payment application forms. There is the ability to generate reports that are used for program management purposes.
  - Fund Manager is the back-end of the application that interacts with FMMI.
- Pro-Tracts' functions include application tracking, production of filled application and contract forms, and access to automatic generation of applicant letters, practice certification, payment approval and filled payment application forms, with the ability to generate reports that are used for program management purposes.

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

- PT-FM does not use any type of tools to analyze PII.

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

- PT-FM does not use 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.

- 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?

- All information contained will be retained in compliance with NARA Guidelines, which vary on average in years from less than one year to more than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017.
- Per the NRCS-1 System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs".

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

- Yes

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

- 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, nonportability of the data and controlled storage of the data located 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?

- PT-FM shares vendor data with National Finance Center (NFC). Vendor name, address, SCIMS ID and bank account details that are created and stored in PT-FM are communicated to NFC, so that the vendor can get paid.
- PT-FM obtains information related to landowners from SCIMS. PT-FM does not share or transmit any information to SCIMS, nor does it update any information in SCIMS.
- PT-FM links to NRCS systems: PRS, OIP, SmarTech CPPEPAC, CMT and CSP.

4.2 How is the information transmitted or disclosed?

- Transmission of information to the NFC is accomplished via secure FTP process through an IPSEC tunnel.
- NRCS has access to a copy of the SCIMS database via replication. Access to the data is through established security rules via eAuth.

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.

- Privacy risks are mitigated by ensuring that access to the data is through established security rules via eAuth and by ensuring that the sharing of sensitive PII with the NFC (which holds such data independently) is only performed by means of secure FTP process through an IPSEC tunnel. 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?

- *N/A*- PII is not shared or disclosed with organizations that are external to the USDA.

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- PII is not shared or disclosed with organizations that are external to the USDA.
- PT-FM, however, is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt
- In addition, PT-FM is subject to the following FSA SORNs: USDA/FSA-2 – Farm Records File (Automated) and USDA/FSA-14 – Applicant/Borrower.

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

- N/A- PII is not shared or disclosed with organizations that are external to the USDA.

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

- Privacy risks are mitigated by virtue of NOT sharing information external to the USDA. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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.

- PT-FM is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

- Yes. NRCS Privacy Policy published on USDA website.

- Yes. FSA Privacy Policy, which states that "Submitting information is strictly voluntary".

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

- The information in PT-FM is based on the rules of the source database. Any PII information is obtained from the SCIMS system, which is maintained by FSA.
- Individuals have a right to consent in accordance with the FSA Privacy Policy and the individual's written consent.

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. Any PII information is obtained from the SCIMS system, which is maintained by FSA. Members of the Public do not have access to this application.

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.

- Any PII information that is obtained from the SCIMS system, is maintained by FSA.

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?

- 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.)."
- Any PII information obtained from the SCIMS system 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 their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

- 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."
- Any PII information obtained from the SCIMS system 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.

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

- The SORN USDA/NRCS-1 is published on the USDA.gov website.
- Any PII information obtained from the SCIMS system 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.

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

- N/A- See section 7.3.

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

- Any PII information obtained from the SCIMS system 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.
- Residual privacy risks associated with the redress process for individuals are mitigated since individuals can use the relevant procedures discussed above to update their original public records.

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?

- Users are authenticated by eAuthentication, the user is directed to the application URL. Access to the website is through a load share switch to one of three Web Servers. PT-FM utilizes a Role Based Access Control (RBAC) model for end-user access to the application. The application has documented Access Control Procedures, in compliance with FISMA and USDA directives. See Section 2.4.

8.2 Will Department contractors have access to the system?

- Yes. Department contractors with a need to know will have access to this application 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.

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 receives information security awareness training before being granted network and account access, which contains the requisite privacy training, and Annual Security Awareness and Specialized Training, as required by FISMA (NIST SP 800-53 rev 4) and USDA policies (USDA OCIO DR 3545-001 – Information Security Awareness and Training Policy and USDA OCIO DR 3505-003 - Access Control Policy).

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

- Yes. PT-FM's most recent authorization to operate (ATO) is dated on 6/18/2019.

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. Additionally, the system provides technical safeguards to prevent misuse of data including:
  - Confidentiality: Encryption is implemented to secure data at rest and in transit for this application (e.g., by FIPS 140-2 compliant HTTPS and end-user hard disk encryption).

- Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).
- Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC). Administrative and management operational controls in place to ensure proper access termination.
- Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: Logging is implemented for this application (e.g. by logging infrastructure).
- Attack Mitigation: The system implements security mechanisms such as input validation.

Notice: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

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?

- PT-FM does not directly collect any PII from any affected landowner (i.e., member of the public), but PT-FM does utilize PII within the system which is obtained from SCIMS, which is maintained by FSA (see Section 1.0 above). 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. Any PII information is obtained from the SCIMS database, copied from the SCIMS system, which is maintained by FSA.
- Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5, and by the security controls discussed in Section 2.4 above. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5, respectively.

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?

- PT-FM is a web-based application housed within the DISC Enterprise Data Center in Kansas City, MO.

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

- No, the project utilizes Agency approved technologies, and these technology choices do not 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?

- *N/A* - Third party websites / applications 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* - Third party websites / applications 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* - Third party websites / applications 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* - Third party websites / applications 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* - Third party websites / applications 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* - Third party websites / applications 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* - Third party websites / applications 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* - Third party websites / applications are not used.

10 Does the system use web measurement and customization technology?

- No, 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?

- *N/A* - See section 10.10.

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.

- PT-FM does not provide access or link to Third Party websites or applications. In addition, the system does not use web measurement or customization technology.

Agency Responsible Officials

JAKE ZEBELL

Digitally signed by JAKE ZEBELL
Date: 2021.03.10 07:47:16 -07'00'

Jake Zebell
ProTractsFundManager Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS

Digitally signed by LANITA THOMAS
Date: 2021.03.03 12:44:13 -05'00'

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

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2021.03.03 08:38:53 -06'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture