

# Privacy Impact Assessment ProTracts/FundManager

Technology, Planning, Architecture, & E-Government

- Version: 2.01
- Date: August 16, 2013
- Prepared for: USDA OCIO TPA&E





# Privacy Impact Assessment for the ProTracts-FundManager

14 August 2013

**Contact Point**

**Deb May**

**Natural Resources Conservation Service**

**970-295-5624**

**Reviewing Official**

**Lian Jin**

**Acting Chief Information Security Officer**

**United States Department of Agriculture**

**202-720-8493**



## Abstract

The ProTracts-FundManager (PT/FM) is a system of the Natural Resources Conservation Service (NRCS).

The Program Contracts System, known as ProTracts-FundManager, is a web-enabled application used to manage NRCS conservation program applications, cost share contracts, and program fund management.

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 Management Act of 2002 (FISMA) and the E-Government Act of 2002 (Public Law. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) Federal Law.

## Overview

The ProTracts-FundManager (PT/FM) is a system of the Natural Resources Conservation Service (NRCS).

The purpose of the ProTracts-FundManager, is to manage NRCS conservation program applications, cost share contracts, and program fund management. ProTracts 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.

ProTracts-FundManager uses the SCIMS ID to access read-only PII information that is shared from the Service Center Information Management System (SCIMS). SCIMS and paper documents are the sources of the PII used in ProTracts-FundManager for the public applicants.

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.

NOTE: ProTracts-FundManager does not process any financial transactions.

This is a legacy application that is hosted on devices using common COTS hardware and software configured in accordance with USDA baseline configurations for servers and web portals.



ProTracts-FundManager shares (receives) PII from the SCIMS database. ProTracts-FundManager shares (transmits) the SCIMS ID and other PII (vendor information) to the NFC.

ProTracts-FundManager interacts with CMT, Customer Service Toolkit, and DMS. ProTracts-FundManager does not share any PII with these applications which are separately accredited.

Authority to operate ProTracts-FundManager was previously provided via the ATO granted in 2010.

## 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?

- No PII is directly collected from any affected member of the public by this application. The PII that is used and maintained by ProTracts-FundManager includes the names and typical contact information for affected individuals (e.g., member of the public) that are referenced in the documents managed by ProTracts-FundManager.
- ProTracts-FundManager uses and maintains information to identify program participants and information to ensure that appropriate payments can be made. The PII that is used/maintained includes the following: name, address, SSN, race, ethnicity, and disability are retrieved from SCIMS and stored in ProTracts. Bank account information is entered into ProTracts / FundManager. Latitude / longitude is calculated based on an area selected on a map and stored in ProTracts.

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

- SCIMS and paper documents are the sources of the PII used in ProTracts-FundManager for the public applicants.

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

- ProTracts-FundManager does not directly “collect” any PII from any affected individual.
- ProTracts-FundManager uses and maintains the PII to support issuing tax dollars to assist NRCS program participants. Legislation mandates participants and their land meet certain eligibility requirements.

### 1.4 How is the information collected?

- ProTracts-FundManager does not directly collect any PII from affected individuals (i.e., members of the Public), nor is PII collected from any other third party sources.

- See 1.2.

### **1.5 How will the information be checked for accuracy?**

- Information in ProTracts-FundManager 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 is not within the scope of ProTracts-FundManager. ProTracts-FundManager 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.

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

While ProTracts-FundManager does not directly “collect” any PII from any individual, these pertain:

- Federal Register /Vol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)
- *NRCS-1 SORN*

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

- ProTracts-FundManager does not directly “collect” any PII from any affected individual (i.e., member of the public).
- This is discussed in the PIA Overview and Section 1.1.
- Privacy risks are mitigated because access to the information will be limited to appropriate NRCS personnel and partners by the use of the USDA-OCIO-eAuthentication application, which provides user authentication for NRCS. Role-Based Access Control (RBAC) provides access enforcement.
- 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.**

- ProTracts-FundManager does not directly “collect” any PII from any affected individual.
- 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. OMB does not approve ProTracts forms since 2012, there is an exception for Farm Bill administration forms
  - Fund Manager is the back-end of the application that interacts with FMML.

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

- N/A – ProTracts-FundManager does not use any type of tools to analyze PII. No PII data is ‘produced’ and PII data is not manipulated or reformatted.

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

- N/A – ProTracts-FundManager 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 Federal Information Security Management Act of 2002 (FISMA) as reflected in CSAM, USDA Office of the Chief Information Officer (OCIO) Directives, and National Institute of Standards and Technology (NIST) guidance, including applicable controls provided in these NIST Special Publication 800-53 control families:
  - Access Control (AC)
  - Audit and Accountability (AU)
  - Security Awareness and Training (AT)
  - Identification and Authentication (IA)
  - Media Protection (MP)
  - Physical and Environmental Protection (PE)
  - Personnel Security (PS)

- Risk Assessment (RA)
- System and Communication Protection (SC)
- System and Information Integrity (SI)

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?

- Application-specific information is retained while the application remains in production. Per NARA General Records Schedule 20, application-specific information has been authorized by the NRCS Records Manager for erasure or deletion when the agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes.

### 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, 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?**

- ProTracts-FundManager obtains information related to affected individuals from SCIMS. Furthermore, ProTracts-FundManager does not share / transmit any information to SCIMS nor does it update any information in SCIMS.
- ProTracts-FundManager receives PII from the SCIMS database, which is maintained in ProTracts-FundManager (the name, address, and SCIMS ID).
- ProTracts-FundManager shares vendor data with NFC. NRCS shares data with NFC and FSA (SCIMS), both of which are USDA organizations.

**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.

**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 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.
- 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 information is not transmitted or disclosed externally.

**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 information is not transmitted or disclosed externally.

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

- N/A – PII information is not transmitted or disclosed externally.

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

- PII information is not transmitted or disclosed externally. Privacy risks are mitigated by virtue of NOT sharing PII with organizations external to 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 Was notice provided to the individual prior to collection of information?**

- N/A – No notice is provided to any affected individual (i.e., member of the public) because no PII is solicited or collected from any individual by this application. *SORN NRCF-1 is applicable.*

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

- N/A – No PII is collected from any affected individual by this application.

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

- N/A – No PII is collected from any affected individual by this application.

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

- Because no PII is collected from any affected individual (i.e., member of the public) by this application, “Notice” does not need to be provided to any individual.
- There is no risk that any affected individual would be unaware of “collection,” because no PII is collected from any individual by this application.

## 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?

- N/A – No procedures are required. PII information in ProTracts-FundManager is not directly available to the individuals themselves (i.e., members of the Public) via this application, because the individuals associated with any PII in the documents maintained in the ProTracts-FundManager are not authorized to gain access to ProTracts-FundManager.
- 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 (owned by the Farm Service Agency), which is the source of some of the PII used by this application.

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

- N/A – No procedures are required. The individuals associated with any PII in the documents maintained in the ProTracts-FundManager are not authorized to gain access to ProTracts-FundManager, so any PII information in ProTracts-FundManager is not directly available to the individuals themselves (i.e., members of the Public) to update or change (i.e., “correct”) any inaccurate or erroneous PII information.
- 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 (owned by the Farm Service Agency), which is the source of some of the PII used by this application.

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

- N/A – no notification is provided related to procedures to allow individuals to correct their PII, because the individuals associated with any PII in the

documents maintained in the ProTracts-FundManager are not authorized to gain access to ProTracts-FundManager.

- No PII is collected from any affected individual by this application.
- 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 (owned by the Farm Service Agency), which is the source of some of the PII used by this application.

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

- N/A – See 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.**

- There are no privacy risks specifically associated with the redress process for this application. There is no risk that an individual would need to correct their PII in ProTracts-FundManager, because no PII is collected from any affected individual by ProTracts-FundManager.
- Residual privacy risks associated with the redress process for individual landowners 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?**

- Access to the ProTracts-FundManagers application is determined via a valid eAuthentication ID and password (level II) on a valid “need to know” basis, determined by requirements to perform applicable official duties. 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 ProTracts-FundManager 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, per General Manual, Title 270, Part 409 - Logical Access Control and Account Management.
- Annual Security Awareness and Specialized Training are also required, per FISMA and USDA policy, and this training is tracked by USDA.

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

- PTFM last received an Authorization to Operate (ATO) in 2010.

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

- NRCS complies with the “Federal Information Security Management Act of 2002” (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. Additionally, NRCS complies with the specific security requirements for “auditing measures and technical safeguards” provided in OMB M-07-16. Finally, 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).
  - 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?**

- ProTracts-FundManager does not directly collect any PII from any affected individual, but ProTracts-FundManager does utilize PII within the system which is obtained from SCIMS and transmitted to NFC (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 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?**

- ProTracts-FundManager is an NRCS legacy application that is seeking an Authorization to Operate (ATO), as discussed in Section 8.4.

**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 3<sup>rd</sup> party websites and/or applications?**

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

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

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

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

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

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

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

**10.6 Is the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications purged periodically?**

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

**10.7 Who will have access to PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications?**

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

**10.8 With whom will the PII that becomes available through the agency’s use of 3<sup>rd</sup> party websites and/or applications be shared - either internally or externally?**



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

**10.9 Will the activities involving the PII that becomes available through the agency's use of 3<sup>rd</sup> party websites and/or applications require either the creation or modification of a system of records notice (SORN)?**

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

**10.10 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 10.10.

**10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3<sup>rd</sup> party websites and/or applications, discuss the privacy risks identified and how they were mitigated.**

- Privacy risks are nominal. ProTracts-FundManager does not provide access or link to 3rd Party Applications. In addition, the system does not use web measurement and customization technology.



## Responsible Officials

deb.may2@usda.  
gov

Digitally signed by  
deb.may2@usda.gov  
DN: cn=deb.may2@usda.gov  
Date: 2013.08.23 15:23:31 -06'00'

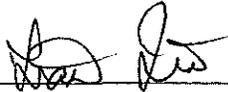
Deb May  
NRCS

Date

United States Department of Agriculture

This signature certifies that the above PIA responses are provided to the best of my knowledge and understanding.

## Approval Signature

  
\_\_\_\_\_

9/6/13  
\_\_\_\_\_

Mr. Lian Jin

Date

Acting Chief Information Security Officer

United States Department of Agriculture

This signature certifies that the PTA analysis and PIA determination due diligence has been conducted pursuant to Department guidance and NIST regulations.