Privacy Impact Assessment
ProTracts/Fund Manager

Technology, Planning, Architecture, & E-Government

- Version: 1.2
- Date: April 26, 2012
- Prepared for: USDA OCIO TPA&E

USDA

United States Department of Agriculture

Privacy Impact Assessment for the

ProTracts/Fund Manager

April 2012

Contact Point
RoopKumar Anikapati
USDA-NRCS
(970) 295-5387

Reviewing Official
Ray Coleman
Director of IT Security
United States Department of Agriculture
(202) 205-7712

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

This Privacy Impact Assessment addresses the security aspects of the Program Contracts system (ProTracts) and its companion system Fund Manager.

ProTracts/Fund Manager is a web-enabled application used by NRCS field office personnel to manage NRCS conservation program applications, cost share contracts, and program fund management for AMA, CSP, EQIP and WHIP. ProTracts/Fund Manager also functions as a "feeder" system to exchange financial transactions with the departmental accounting system known as the Federal Financial Information System (FFIS).

This PIA is being conducted due to a departmentally mandated initiative to implement a new accounting system called the Financial Management Modernization Initiative (FMMI) and will impact the interfaces within ProTracts/Fund Manager.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

The Program Contracts System, known as ProTracts, is a web-enabled application used by NRCS field office personnel to manage NRCS conservation program applications, cost share contracts, and program fund management for AMA, CSP, EQIP, and WHIP. ProTracts is used

to manage funds allocated from Financial Management Modernization Initiative (FMMI) 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 for program participants by electronic fund transfer from FMMI.

Fund Manager is a companion system to ProTracts. Fund Manager application handles the vendor master data for ProTracts purposes and it interfaces with FMMI for vendor updates. For purposes of C&A, ProTracts and Fund Manager are grouped together. For purposes of PIAs, the two systems are grouped together. Conservation Management Tool (CMT) and the ProTracts Ranking Tool are also components of ProTracts system designed for ranking applications.

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 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 and standard data queries built into many contracting work flows. Contracts are established using state developed cost lists or payment schedules which are maintained in the electronic Field Office Technical Guide (eFOTG).

ProTracts is integrated with Farm Service Agency (FSA) web services to enforce payment limitations, adjusted gross income limits (AGI), and participant eligibility determinations.

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?

ProTracts/FundManager, as a feeder system to FMMI, collects, uses, disseminates and/or maintains SSNs, TINs, Bank Routing and Bank Account Numbers, Customer Names, Customer (potential Program participants) Addresses, Customer Property Latitude and Longitudinal coordinates, SCIMS IDs, and Contract numbers.

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

Sources of information include SCIMS, other FSA web services, Customer Service Toolkit

(CST), potential and existing program participants. Program participants include landowners, operators, producers, cooperators.

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

ProTracts/FundManager issues tax dollars to assist program participants. Legislation mandates participants and their land meet certain eligibility requirements.

1.4 How is the information collected?

SCIMS, other FSA web services, and Customer Service Toolkit (CST), provide data to ProTracts/Fund Manager through web services. Program participants also provide information through an application process and payment request process.

1.5 How will the information be checked for accuracy?

Data sources include other USDA and IRS sources. The data collected from USDA sources is trusted and not verified by NRCS. NRCS employees validate data with the participant either verbally or in writing through the use of form CPA-1200 and submits the tax-id and banking information in the form of a vendor transaction that is validated against IRS records and Federal Reserve bank routing information.

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

SORN

The Statement of Record attributes the authority for maintenance of the system as 16 U.S.C 590 a-f, q, q-l and other applicable authorities.

PRIVACY ACT STATEMENT
The following statement is made in accordance with the Privacy Act of 1974 (5 USC 552a). This information is used to track contract or agreement progress. The authority for requesting the following information is 7 CFR 630 (Long Term Contracting); 7 CFR 1410 (CRP); 7 CFR 631 and 702 (IEQIP); 7 CFR 636 (WHIP); 7 CFR 622 (WPFPP); 7 CFR 1465 (AMA); 7 CFR 1469 (CSP); 7 CFR 625 (HFR); 7 CFR 1494 (FRPP); and 7 CFR 1467 (WRP). Furnishing information is voluntary and will be confidential; however, it is necessary in order to receive assistance.

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

Only certain roles have the permission in ProTracts to view collect or maintain PII data in ProTracts/FundManager. Banking information is masked when displayed by other roles with insufficient permissions. Masking is done by the front-end application. Data containing PII is always encrypted and password protected. Masking is used to protect the SSNs and TINs.

The design of this application ensures that only the minimum required amount/type of data is collected to meet the requirement of distributing funds to the requesting public. The customer information is stored in a secure SQL Server database in the USDA enterprise data center in Kansas City. This system is secure (i.e., uses secure https protocol). HTTPS is another design element which ensures this system merits a moderate classification.

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/Fund Manager is a web-enabled application used by NRCS field office personnel to manage NRCS conservation program applications, cost share contracts, and program fund management for AMA, CSP, EQIP and WHIP. ProTracts/Fund ~~Manager also~~Manager ~~functions~~also functions as a "feeder" system to exchange financial transactions with the departmental accounting system known as the Financial Management Modernization Initiative (FMMI)).

ProTracts is also used to manage funds allocated from Financial Management Modernization Initiative (FMMI) 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 for program participants by electronic fund transfer from FMMI. Fund Manager is a companion system to ProTracts. Fund Manager application handles the vendor master data for ProTracts purposes and it interfaces with FMMI for vendor updates. For purposes of C&A, ProTracts and Fund Manager are grouped together. For purposes of PIAs, the two systems are grouped together. Conservation Management Tool (CMT) and the ProTracts Ranking Tool are also components of ProTracts system designed for ranking applications.

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 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 and standard data queries built into many contracting work flows.

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

ProTracts/FundManager produces a number of standard reports accessible to field personnel to allow then to analyze data. Database queries are sometimes conducted to provide detailed data to resolve individual problem, or to provide headquarters with information to respond to congressional inquiries, and to perform program analysis.

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

No publicly available data in included.

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.

System access is restricted to authorized Natural Resources Conservation Service employees and conservation district employees and technical service providers working to assist with the implementation of natural resources programs. NRCS field employees are authorized to access system records of landowners, operators, producers, cooperator, or participants in their service area or outside of their service area if the landowner, operator, producer, cooperator, or participant has authorized access. Conservation district employees are authorized to access system records of their district landowners, operators, producers, cooperators, or participants only in their official capacity as district employees.

The electronic data retrieval system is secured by the USDA Common Computing Environment user authentication process and USDA eAuthentication login and password protection. Hardcopy files are maintained in file cabinets, which should be locked when not in use. Offices are locked during non-business hours.

Password protection and encryption of data are routinely used to protect data in transit. Access to reports requires authentication and a role having sufficient permission.

A separate Administration Application provides strong access controls to prevent unauthorized access to the PII data in the system, via Level 2 eAuth.

Section 3.0 Retention

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

3.1 How long is information retained?

Records are maintained as long as the landowner, operator, producer, cooperator, 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)?

Refer to GM-120 408 Part A & B for policy regarding record retention. Disposal is TBD (and may currently be indefinite). Retention period is consistent with requirements given at: http://www.archives.gov/about/laws/disposal-of-records.html#lists

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 risks associated with this application are MODERATE due to the sensitive PII collected and stored.

This is MODERATE because the risks that exist related to this PII are mitigated by the design of this application, which ensures that only the minimum required amount/type of data is collected to meet the requirement of distributing funds to the requesting public.

SSNs, TINs, and banking/financial information is sensitive PII. The ability to track the individual and potentially said individual's finances may not be limited despite the customer information being stored in a secure SQL Server database in the USDA NITC enterprise data center in Kansas City.

This Information System (i.e. this application) is hosted by ITS, and is covered by the ITS Service Level Agreement (SLA) that has been uploaded in CSAM— ProTracts/FundManager is under Conservation Program Delivery (CPD) in CSAM.

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?

Programs Deputy Area – to analyze program data

Financial Management Deputy Area – to analyze financial data

REAP Team – for Congressional Reporting

Field Staff, Technical IT Staff – to analyze and resolve problems

Any information sharing outside of the NRCS Information Technology Center (ITC) requires a special Data Request be submitted to Director of IT Security for approval. This request details the types and quantities of data to be extracted and the intended use and must be approved prior to an extract. Information is shared via aggregate for special reports.

4.2 How is the information transmitted or disclosed?

Primarily, information is transmitted through the application in the form of reports. When necessary, custom data queries are executed to extract data which is encrypted, password protected, and copies to an SFTP server for pick-up. It is still strictly NRCS use.

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.

Internally, every NRCS employee has the responsibility to protect sensitive information. There is no external information sharing.

Risks may include the internal threat—are all people handling PII appropriately? Human error and natural disasters are also risks.

Users must supply a valid eAuthentication user ID and password to access the Fund Manager system. Once the user is successfully authenticated, credentials are passed through SiteMinder and IdentityMinder in order to identify where the user is coming from (public, NRCS, state/local offices, etc.) and the to zRoles to determine what information the user is permitted to access.

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?

ProTracts does not share information with non-USDA entities. - There is no external information sharing from the ProTracts/FundManager application.

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.

Again, there is no external information sharing from the ProTracts/FundManager application. The applicable SORN would be NRCS-1.

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

Per 5.2, no external sharing occurs. If a business requester makes a data extract request, any special Data Request and Disclosure Form is submitted to the Director of IT Security for approval. This request details the types and quantities of data to be extracted and the intended use and must be approved prior to an extract.

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

Any information sharing outside of the NRCS Information Technology Center (ITC) requires a special Data Request be submitted to Director of IT Security for approval. This request details the types and quantities of data to be extracted and the intended use and must be approved prior to an extract.

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?

The CPA-1200 'Conservation Program Application' includes the privacy statement. The potential participant must complete, read, and acknowledge the information contained in the form in order to apply for one of the programs administered in ProTracts/FundManager. Customer receives the CPA-1200 application... The application with the form becomes source document within ProTracts. Notice is provided on form via field office personnel.

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

No, completion of the form is a requirement in order to participate in a program.

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

No, completion of the form is a requirement in order to participate in a program.

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.

The CPA-1200 'Conservation Program Application' and SF-1199'Direct Deposit Sign up Form' (bank form for electronic fund transfers (EFT)). are required for program participation and require customer certification.

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?

Any individual may obtain information as to the procedures for gaining access to 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.

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

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.

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

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.). The government will, in turn, respond to this request (with the individual's address included in the correspondence to the government).

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

Formal redress is provided pursuant to Sections 7.1 and 7.2.

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

The mitigations associated with redress are the same as with the data initially provided.

Programmers to provide Tier 3 support. Risk is mitigated by requirement that programmers/users be on the USDA network backbone, using a CCE computer, with valid eAuthentication and zRoles credentials. Also, separation of duties, auditable events mitigate risk.

Use of External Information Systems (1) - The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system (Incorporated from the Security RTM Report, p. 5).

Security Awareness and Training Policy and Procedures - The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls (Incorporated from the Security RTM Report, p. 5).

Other risks may include wireless vulnerabilities. Also, contingency planning and procedure may not be comprehensive and fully effective. Risks may also include environmental hazards (Incorporated from the Security RTM Report, p. 4, 11, 26).

Local Registration Authorities (LRAs) are USDA employees who are trained to act as the trusted entity to validate the identity of a customer seeking a level 2 eAuthentication account. The role of the LRA can be compared to a Notary Public who ensures the identity of an individual conducting official business transactions. This process is called "identity proofing". Training and a list of approved forms of photo identification for Identity proofing Services for USDA eAuthentication mitigate this risk. Limited access controlled for users as users must have an established account.

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?

Policy states: The state conservationists (STC) will use Form AD-1143, "Corporate Systems Access Request Form," to delegate contracting responsibilities and authorize appropriate individuals to assign the appropriate roles in ProTracts and fund manager. Form AD-1143 will be used to document the request and approval of each action to add, delete, or modify

user roles. There must be complete separation of duties between the user requesting access, the supervisor who approves the access, and the role grantor who enrolls the user. The fund manager State vendor coordinator and fund manager obligation approver roles may only be enrolled by the designated national financial role grantor. All Forms AD-1143 forms must be maintained by the approving supervisor and role grantor following the filing and disposition policy contained in the NRCS records guide, located in 120-GM, Part 408, Subpart D, "Records Guide," under file code 250-11.

Role based access limits those viewing sensitive PII. The sensitive PII (e.g., social security numbers collected in this system) must be masked/eliminated/encrypted…

8.2 Will Department contractors have access to the system?

Yes, Agency contractors will have access to the system..

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

Privacy training for all employees and contractors was provided through Aglearn.

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

ProTracts/FundManager last certification and accreditation renewal was completed in 2009.

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

All data requests are submitted in writing, and approved by the NRCS Security Officer before fulfilling the request. Encrypted network and time out are also used.

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?

A risk is unauthorized disclosure of sensitive PII. We mitigate this risk by require access only through a government computer connected to the USDA backbone by authorized representatives.

The risks associated with this application are MODERATE due to the sensitive PII collected and stored.

This is MODERATE because the risks that exist related to this PII are mitigated by the design of this application, which ensures that users may gain access to only the minimum required amount/type of data is collected to meet the requirement of distributing funds to the requesting public.

Sensitive data is masked for most users. Data is encrypted and password protected in transit. The application will timeout after a period of inactivity. Separation of Duties is enforced.

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 a feeder system that produces transactions used by the USDA department-wide accounting system (FMMI).

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

No. ProTracts/FundManager is a feeder system that produces transactions used by the USDA department-wide accounting system (FMMI).

ProTracts/Fund Manager has not implemented any technology that would 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"?

The ProTracts/Fund ManagerPproject Manager has reviewed both documents.

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

ProTracts/FundManager does not use 3rd party websites.

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

ProTracts/FundManager does not use 3rd party websites.

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

ProTracts/FundManager does not use 3rd party websites.

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?

ProTracts/FundManager does not use 3rd party websites.

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

ProTracts/FundManager does not use 3rd party websites.

If so, is it done automatically?

ProTracts/FundManager does not use 3rd party websites.

If so, is it done on a recurring basis?

ProTracts/FundManager does not use 3rd party websites.

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

ProTracts/FundManager does not use 3rd party websites.

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?

ProTracts/FundManager does not use 3rd party websites.

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)?

ProTracts/FundManager does not use 3rd party websites.

10.10 Does the system use web measurement and customization technology?

ProTracts/FundManager does not allow users to customize settings.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

ProTracts/FundManager does not allow users to customize settings.

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?

ProTracts/FundManager does not allow users to customize settings

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

ProTracts/FundManager **does not allow users to customize settings.**

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.

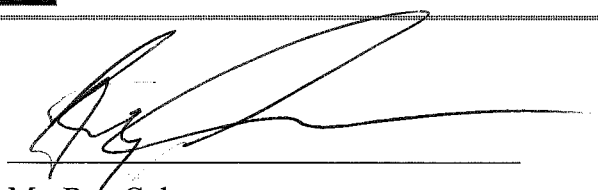
ProTracts/FundManager does not allow users to customize settings. ProTracts does not use 3rd party websites.

Responsible Officials

RoopKumar Anikapati, Project Manager

United States Department of Agriculture

Approval Signature



Mr. Ray Coleman
Director of IT Security
United States Department of Agriculture