



Privacy Impact Assessment

Office Information Profile (OIP)

Revision: 1.0

*Natural Resources Conservation Service
(NRCS)*

Date: November, 2009



Document Information

Owner Details	
Name	Kathy Green, Branch Chief, USDA-NRCS-ITC
Contact Number	(970) 295-5647
E-mail Address	Kathy.Green@ftc.usda.gov

Revision History			
Revision	Date	Author	Comments
1.0	11/4/2009	K. Hennings	Verify and transfer information into the new template

Distribution List			
Name	Title	Agency/Office	Contact Information



Table of Contents

DOCUMENT INFORMATION	II
TABLE OF CONTENTS	III
1 SYSTEM INFORMATION	1
2 DATA INFORMATION	2
2.1 Data Collection	2
2.2 Data Use	3
2.3 Data Retention	4
2.4 Data Sharing	4
2.5 Data Access	5
2.6 Customer Protection	6
3 SYSTEM OF RECORD	8
4 TECHNOLOGY	8
5 COMPLETION INSTRUCTIONS	9



1 System Information

System Information	
Agency:	USDA - NRCS
System Name:	Office Information Profile (OIP)
System Type:	<input type="checkbox"/> Major Application <input type="checkbox"/> General Support System <input checked="" type="checkbox"/> Non-major Application
System Categorization (per FIPS 199):	<input type="checkbox"/> High <input checked="" type="checkbox"/> Moderate <input type="checkbox"/> Low
Description of System:	The Office Information Profile (OIP) system provides comprehensive office information for Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), Rural Development (RD) offices, plus partner organization offices. This information identifies office locations, the agencies present, mailing and shipping addresses, phone numbers, and agency representatives designated as points of contact. OIP also serves as an interface with the public, allowing easy access to contact information for any service center office (SCO) or Service Center Agency (SCA) partner site.
Who owns this system? (Name, agency, contact information)	Kathy Green, Branch Chief – USDA – NRCS – ITC Kathy.Green@ftc.usda.gov (970) 295-5647
Who is the Project Manager for this system? (Name, agency, contact information)	Paige Niederer, Project Manager – USDA – NRCS – ITC Paige.Niederer@ftc.usda.gov (970) 295-5496
Who is the security contact for this system? (Name, agency, contact information)	Chuck Hart, Information System Security Manager (ISSM) USDA – NRCS – ITC Chuck.Hart@ftc.usda.gov (970) 295-5550
Who completed this document? (Name, agency, contact information)	Kimberly Hennings, Systems Security Analyst USDA – NRCS – ITC (Contractor) Kim.Hennings@ftc.usda.gov (970) 295-5428



2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	The Office Information Profile (OIP) system provides comprehensive office information for Farm Service Agency (FSA), Natural Resources Conservation Service (NRCS), Rural Development (RD) offices, plus partner organization offices. This information identifies office locations, the agencies present, mailing and shipping addresses, phone numbers, and agency representatives designated as points of contact. OIP also serves as an interface with the public, allowing easy access to contact information for any service center office (SCO) or Service Center Agency (SCA) partner site.
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	N/A
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
4	Sources of the data in the system.	N/A
4.1	What data is being collected from the customer?	Data is not being collected from customers.
4.2	What USDA agencies are providing data for use in the system?	Conservation Districts and various State and Local agencies co-located with USDA service centers.
4.3	What state and local agencies are providing data for use in the system?	State Farm Committee (FAC)
4.4	From what other third party sources is data being collected?	None
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 6.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	N/A Data is not being collected from customers.



No.	Question	Response
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	All data is verified by the State Farm Committee (FAC).
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	All data is verified by the State Farm Committee (FAC).

2.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	OIP provides office location, business contact information and asset tracking information and does not collect information about individuals.
7	Will the data be used for any other purpose?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 8.
7.1	What are the other purposes?	N/A
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 10.
9.1	Will the new data be placed in the individual's record (customer or employee)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No N/A
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No N/A
9.3	How will the new data be verified for relevance and accuracy?	All data is verified by the State Farm Committee (FAC).
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	OIP provides office location, business contact information and asset tracking information and does not collect information about individuals.
11	Will the data be used for any other uses (routine or otherwise)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 12.
11.1	What are the other uses?	N/A



No.	Question	Response
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	N/A
13	Are processes being consolidated?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 14.
13.1	What controls are in place to protect the data and prevent unauthorized access?	N/A

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	Indefinitely.
14.2	What are the procedures for purging the data at the end of the retention period?	N/A
14.3	Where are these procedures documented?	N/A
15	While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	Data stewards for the OIP application have been designated and are responsible for ensuring all data is up-to-date and accurate.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No

2.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No – If NO, go to question 18.



No.	Question	Response
17.1	How will the data be used by the other agency?	Data will be used by the agency to provide comprehensive office and assets tracking information for Farm Service Agency, Natural Resource Conservation Service, OCIO-ITS, Rural Development.
17.2	Who is responsible for assuring the other agency properly uses the data?	NRCS owns and maintains the OIP application.
18	Is the data transmitted to another agency or an independent site?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 19.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	N/A
19	Is the system operated in more than one site?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	N/A

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	<ul style="list-style-type: none"> NRCS, RD, FSA and OCIO-ITS users will have access to data within the OIP application. (The term users also includes managers) System administrators (Also know as Data Stewards) will have access to data within the OIP application. General Public – will have access to contact information for any service center office (SCO) or Service Center Agency (SCA) partner site.
21	How will user access to the data be determined?	<ul style="list-style-type: none"> The OIP application users may include anyone within NRCS, RD, OCIO-ITS and FSA agencies with a valid need to know. OIP Data Stewards whose job responsibilities require a need for OIP system data access. Select information is also provided to the general public for Web browser viewing. (No access determination is needed for public access).
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No



No.	Question	Response
22	How will user access to the data be restricted?	Users are authenticated via eAuthentication and authorized via a valid need to know and local and national data steward.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

2.6 Customer Protection

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	OIP does not collect or maintain customer data. However, NRCS owns and maintains the OIP application and would be responsible for protecting the privacy right of employees affected by the interface. NOTE: per the table above on page 2 of 11 information such as: Name, email address, telephone number and street address is considered PII information and warrant a PIA. Additionally OIP only publishes employee business contact information



Privacy Impact Assessment for OIP

No.	Question	Response
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	<p>If incident response assistance is needed Customers and employees can contact the NRCS Security Response Team via the following numbers:</p> <ul style="list-style-type: none"> • Lost and Stolen equipment NRCS 800 number (1-888-926-2373) and/or e-mail address (nrcs.security@usda.gov). • Personal Identifiable Incidents – 877-744-2968 (PII-2YOU) • NRCS/CD - (202) 757-8111 or (703) 200-3008 <p>Additionally, each state has an Information System Security Point of Contact (ISSPOC) and a State Administrative Officer (SAO) that can be contacted at their Center or State Office. Furthermore, NRCS leverages incident response assistance from the USDA Cyber Security. The USDA Cyber Security provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.</p>
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	<input checked="" type="checkbox"/> Yes – If YES, go to question 27. <input type="checkbox"/> No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	N/A
27	Consider the following: <ul style="list-style-type: none"> ▪ Consolidation and linkage of files and systems ▪ Derivation of data ▪ Accelerated information processing and decision making ▪ Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	N/A
28	How will the system and its use ensure equitable treatment of customers?	OIP does not collect or maintain customer data.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 30



No.	Question	Response
29.1	Explain	N/A

3 System of Record

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	N/A
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov .)	N/A
30.3	If the system is being modified, will the SOR require amendment or revision?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No N/A

4 Technology

No.	Question	Response
31	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No – If NO, the questionnaire is complete.
31.1	How does the use of this technology affect customer privacy?	N/A

5 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF
INFORMATION OFFICE FOR CYBER SECURITY.



Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

System Manager/Owner
OR Project Representative
OR Program/Office Head.

Date

Agency's Chief FOIA officer
OR Senior Official for Privacy
OR Designated privacy person

Date

Agency OCIO

Date