USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: **Food and Nutrition Service, USDA**

System Name: **Regional Office Administered Program (ROAP) Payment System**

System Type: **Major Application**

System Categorization (per FIPS 199):

Moderate

Description of the System:

The ROAP Payment System is a web-based system which allows recipient organizations (RO's) participating in our ROAP to enter claims for reimbursement and applications for participation online. The system stores information unique to each RO, accepts the claims for reimbursement, calculates each RO's reimbursement, runs paylists and generates a number of reports.

Who owns this system? (Name, agency, contact information)

Catherine Lueck, Regional Director, Financial Management
Mid-Atlantic Regional Office
Food and Nutrition Service, USDA
609-259-5020
Catherine.lueck@fns.usda.gov

Who is the security contact for this system? (Name, agency, contact information)

Robert Speary, Regional IT Security Manager
Mid-Atlantic Regional Office
Food and Nutrition Service, USDA
609-259-5067
Robert.Speary@fns.usda.gov

Shawn Jones, Acting Information Systems Security Program Manager
Headquarters
Food and Nutrition Service, USDA
703-305-2528
Shawn.Jones@fns.usda.gov

Who completed this document? (Name, agency, contact information)

Howard Lockstein, Team Leader
Mid-Atlantic Regional Office
Food and Nutrition Service, USDA
609-259-5170
Howard.lockstein@fns.usda.gov

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	Yes	No
Social Security Number	No	No
Telephone Number	Yes *	No
Email address	Yes *	No
Street address	Yes *	No
Financial data	No	No
Health data	No	No
Biometric data	No	No
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code[1]	No	No
Are social security numbers embedded in any field?	No	No
Is any portion of a social security numbers used?	No	No
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	No	No

*** Telephone number, email address, and street address are related to the organization and not an individual.**

If all of the answers in Questions 1 and 2 are NO, STOP

You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

DATA COLLECTION

3. Generally describe the data to be used in the system.

Information on recipient agencies includes general information such as address, names of responsible officials, user ID and password, number of sites, programs in which the RO participates, enrollment and average daily attendance, numbers of eligible children, bank routing information, history of meal claims and payments.

4. 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.

Yes

5. Sources of the data in the system.

5.1. What data is being collected from the customer?

Data that is collected from the RO includes the address, names of responsible officials, number of sites, programs in which the RO participates, enrollment and average daily attendance, numbers of eligible children, days of operation, bank routing information, history of meal claims and payments, etc.

Sources of information come from two categories:

1. Data input by the FNS user that he/she derives from submitted forms and information gathered by the user or the user's agents.
2. Data input by a participating RA that has appropriate agreements with FNS. This data is always reviewed and approved by FNS.

5.2. What USDA agencies are providing data for use in the system?

The Food and Nutrition Service

5.3. What state and local agencies are providing data for use in the system?

Local recipient agencies which have agreements with FNS, including schools, child and adult day care centers, Summer Food Service Program sites, and residential child care institutions.

5.4. From what other third party sources is data being collected?

None

6. Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

Yes, customers (ROs)

6.1. How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?

Online edit checks and validation of some information by FNS staff through desk review and onsite visits.

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

N/A – All data is collected from customers (Recipient Organizations)

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?

N/A – All data is collected from customers (Recipient Organizations)

DATA USE

7. 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?

The data is used to gather program information on eligible recipient organizations to approve them to participate in FNS' programs and to provide reimbursement.

8. Will the data be used for any other purpose?

No. If NO, go to question 9

8.1. What are the other purposes?

9. 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

Yes

10. 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.)?

No

10.1. Will the new data be placed in the individual's record (customer or employee)?

N/A

10.2. Can the system make determinations about customers or employees that would not be possible without the new data?

N/A

10.3. How will the new data be verified for relevance and accuracy?

N/A

11. 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?

The data is used to verify the recipient organization's eligibility to participate and the value of reimbursement payments for the Child Nutrition Programs.

12. Will the data be used for any other uses (routine or otherwise)?

No. If NO, go to question 13

12.1. What are the other uses?

13. 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?

Yes

13.1. What controls are in place to protect the data and prevent unauthorized access?

- Electronic access to the servers is protected by FNS/USDA firewalls and network security.
- The application is protected by authorization and authentication at the application level.
- Intrusion detection devices will monitor the servers that are available to the public.
- EIN data is stored encrypted in the database.

14. Are processes being consolidated?

Yes

14.1. What controls are in place to protect the data and prevent unauthorized access?

The controls will remain in place via the applications implementation of security privileges at the role and individual level.

DATA RETENTION

15. Is the data periodically purged from the system?

Yes

15.1. How long is the data retained whether it is on paper, electronically, in the system or in a backup?

Dat a is retained for three years on-line and then stored for 3 years off-line after the cutoff (end of fiscal year).

15.2. What are the procedures for purging the data at the end of the retention period?

Del etion will take place at least annually.

15.3. Where are these procedures documented?

Is in draft form and will be included in the ROAP procedures.

16. 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?

Relevant program data is updated annually during application renewal process.

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

Yes

DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

No. If NO, go to question 19

18.1. How will the data be used by the other agency?

18.2. Who is responsible for assuring the other agency properly uses of the data?

19. Is the data transmitted to another agency or an independent site?

Yes

19.1. Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

Yes

20. Is the system operated in more than one site?

No. If NO, go to question 21

20.1. How will consistent use of the system and data be maintained in all sites?

DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

The users of the system are eligible recipient organizations (RO) and FNS employees. RO users have the ability to enter claims data and program information for their operation and have view capabilities in other areas. FNS employees have varying degrees of accessibility according to their user roles, including the ability to update or view the data.

22. How will user access to the data be determined?

Access to the system is given according to existing FNS processes which includes the submission of an FNS 674 "Computer System Access Request" form.

22.1. Are criteria, procedures, controls, and responsibilities regarding user access documented?

Yes

23. How will user access to the data be restricted?

Access to the data is determined according to the user's role. Recipient organizations only have access to their own data. FNS users have view only rights for all aspects and have the ability to modify data according to their function (application specialist, application manager, financial etc…)

23.1. Are procedures in place to detect or deter browsing or unauthorized user access?

Yes

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

Yes

CUSTOMER PROTECTION

25. 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.)?

N/A

26. How can customers and employees contact the office or person responsible for protecting their privacy rights?

N/A

27. 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?

Yes. If YES, go to question 28

27.1. If NO, please enter the POAM number with the estimated completion date:

28. Consider the following:

- 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)?

No. If NO, go to question 29

28.1. Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of customers?

The system can be used to monitor the participation of eligible recipient organizations according to the policies and relevant laws that govern their participation.

30. Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?

No. If NO, go to question 31

30.1. Explain

SYSTEM OF RECORD

31. 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?

Yes

31.1. How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

Recipient organizations are assigned a unique five digit number. Data is retrieved using this number.

31.2. Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov)

N/A

31.3. If the system is being modified, will the SOR require amendment or revision?

N/A

TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

No. If NO, the questionnaire is complete.

32.1. How does the use of this technology affect customer privacy?

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/CYBER SECURITY

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

ROAP
(System Name)

This document has been completed in accordance with the requirements of the EGovernment 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.

Catherine Smith — 6/28/2007

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