USDA Rural Development

Committed to the future of rural communities.

Privacy Impact Assessment

For

Multi-Family Management

Automated Multi-Housing Accounting System (AMAS)

Multi Family Integrated System (MFIS)

Management Interactive Network Connection (MINC)

Version 1.0

April 2007

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Multi-Family Management System. This document has been completed in accordance with the requirements of the E-Government Act of 2002.

MANAGEMENT CERTIFICATION – Please check the appropriate statement.

X The document is accepted.

________ The document is accepted pending the changes noted.

________ The document is not accepted.

____ **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.

Glen Boeckmann System Manager - Glen Boeckmann	5-25-07 DATE
OCIO/Project Representative - Eugene Texter	5-25-07 DATE
Peggy Stroud Program/Office Head – Peggy Stroud	6/6/07 DATE
OCIO – John Distler	6/6/07 DATE
Brenda Dinges Chief FOI/PA – Brenda Dinges	6/10/07 DATE
Senior Official for Privacy – Christopher L. Smith	6/6/07 DATE

Table of Contents

Name of Project: Multi Family Management (MFM)
Program Office: Rural Development
Project's Unique ID: 005-55-01-01-01-1010-00-402-129

Information System Name/Title	Multi-Family Management System
System Acronym	MFM
System of Records (SOR)	USDA / RD-SOR-1
System Type	☐ ***GSS*** ☒ ***MA*** ☐ ***GSS sub-system*** ☐ ***MA individual application***
Responsible Organization	USDA – Rural Development

A. CONTACT INFORMATION

1. Who is the person completing this document?

Name	Glen Boeckmann
Title	Chief, Management Services Technologies Branch
Address	USDA Rural Development 1520 Market Street St. Louis, MO 63103
Email address	glennon.boeckmann@stl.usda.gov
Phone Number	314-335-8598

2. Who is the system owner?

Name	Peggy Stroud
Title	Director, Systems Design and Development Division
Address	USDA Rural Development 1520 Market Street St. Louis, MO 63103
Email address	Peggy.stroud@stl.usda.gov
Phone Number	314-335-8925

3. Who is the system manager for this system or application?

Name	Glen Boeckmann
Title	Chief, Management Services Technologies Branch
Address	USDA Rural Development 1520 Market Street St. Louis, MO 63103
Email address	glennon.boeckmann@stl.usda.gov
Phone Number	314-335-8598

4. **Who is the IT Security Manager who reviewed this document?**

Name	Eugene Texter
Title	Information Security Staff Team Lead
Address	USDA Rural Development 1520 Market Street St. Louis, MO 63103
Email address	eugene.texter@stl.usda.gov
Phone Number	314-335-8104

5. **Did the Chief FOI/PA review this document?**

Name	Brenda Dinges
Title	Information System Security Program Manager
Address	USDA Rural Development 1520 Market Street St. Louis, MO 63103
Email address	brenda.dinges@stl.usda.gov
Phone Number	314-335-8829

6. **Did the Agency's Senior Office for Privacy review this document?**

Name	Christopher L. Smith
Title	Rural Development CIO
Address	300 7th ST SW Washington DC 20024
Email address	ChristopherL.Smith@wdc.usda.gov
Phone Number	202-692-0212

7. **Who is the Reviewing Official?** (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).

Name	Christopher L. Smith
Title	Rural Development CIO
Address	300 7th ST SW Washington DC 20024
Email address	ChristopherL.Smith@wdc.usda.gov
Phone Number	202-692-0212

B. SYSTEM APPLICATION/GENERAL INFORMATION

Multi Family Management (MFM) is a Multi Family Housing (MFH) line of business that includes all of the information systems for making and servicing MFH loans and grants. It is a mission-critical CPIC system with a FIPS 199 security rating of "moderate." The three components of MFH are Automated Multi-Family Account System (AMAS) hosted on the NITC mainframe, Multi-Family Integrated System (MFIS) and Management Agent Interactive Network Connection System (MINC) hosted on the St. Louis Web Farm.

1. Does this system contain any information about individuals?	**AMAS Customer Information**: Management agent, borrower names, social security numbers and Borrower debt payment information. **MFIS Customer Information**: Management agent, borrower and key member names and social security numbers. Borrower debt payment information. Project housing unit and rent information. **MFIS Tenant Information**: Tenant household information including name, social security numbers and financial information. **MINC:** This system is a display and collection system for the data held in the Multi Family Integrated System (MFIS). It does not store or maintain any data unique to the application. See the MFIS response for a description of the data displayed and or collected.
(a) Is this information identifiable to the individual? (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed past this section.	**AMAS:** Yes – Management Agents if Individuals and Borrowers if Individuals. **MFIS:** Yes – Tenant Information, Management Agents if Individuals, Borrowers if Individuals, and Key Members. **MINC:** This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application. See the MFIS response for a description of the data displayed and or collected.
(b) Is the information about individual members of the public?	Yes
(c) Is the information about employees?	No
2. What is the purpose of the system/application?	**AMAS:** AMAS provides online transaction entry, batch processing and inquiry support for accounting, financial management and management information purposes for Rural Development servicing offices, State Offices, National Office and the Finance Office. **MFIS:** MFIS is one of USDA's official accounting support systems for the Multi-Family Housing program in Rural Development. MFIS is an online transaction entry and inquiry support system accessed by over 200 field offices, the National Office, and Finance Office. **MINC:** MINC is one of USDA's official accounting support systems for the Multi-Family Housing (MFH) program in Rural Development. MINC is an online

	transaction entry, transmission and inquiry support system accessed by over 7,000 external trusted partners (MFH Management Agents).
3. What legal authority authorizes the purchase or development of this system/application?	OMB Exhibit 300

C. DATA in the SYSTEM

1. Generally describe the type of information to be used in the system and what categories of individuals are covered in the system?	**AMAS Customer Information**: Client names, Social Security Numbers of Borrowers, Co-Borrowers, Key Members addresses, and business financial data, debt payment information. **MFIS Customer Information**: Management agent, borrower and key member names and social security numbers. Borrower debt payment information. Project housing unit and rent information. **MFIS Tenant Information**: Tenant household information including name, social security numbers and financial information. **MINC Customer Information**: Management agent, borrower and key member names and social security numbers. Borrower debt payment information. Project housing unit and rent information. **MINC Tenant Information**: Tenant household information including name, social security numbers and financial information.
2. What are the sources of the information in the system?	**AMAS:** Rural Development field office personnel collect the Loan Obligation information from prospective Borrowers/Applicants. Rural Development field office employees using data entry screens then enter the data into AMAS for batch processing. No external partners have access to the AMAS data. **MFIS:** Management agents who manage the properties of borrowers provide tenant status information to Rural Development. This information is received in separate data files transmitted through the MINC system. Also, data entry screens are completed via the web by RD Area Specialists for borrowers who do not participate through MINC. Batch feeds are obtained nightly from the AMAS mainframe system for borrower and project detail information. **MINC:** Tenant status information is provided to Rural Development by management agents who manage the

	properties of borrowers. This information is received in separate data files transmitted through the MINC system. Also, data entry screens are completed via the web by RD Area Specialists for borrowers who do not participate through MINC.
(a). Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?	**AMAS:** The information is collected from the individual. **MFIS, MINC:** Source of the tenant Information is from the Individual as reported on the application to the management agent.
(b). What Federal Agencies are providing data for use in the system?	**AMAS:** USDA Rural Development loan officers for entering obligation and servicing data. Trusted Management Agents for entering loan payment information into MINC that is fed to AMAS for update. **MFIS:** USDA Area Specialists for inputting tenant and budget information not received via MINC. Trusted Management Agents for inputting tenant and budget information via MINC. RD Finance Office inputting loan information into AMAS received via nightly downloads. **MINC:** NONE
(c). What State and Local Agencies are providing data for use in the system?	NONE
(d). From what other third party sources will data be collected?	**AMAS:** NONE **MFIS, MINC:** Data transmitted in ASCII File format through Gentran product from Management Agents/Service Bureaus Vendor Software.
(e). What information will be collected from the customer/employee?	**AMAS:** Information included contains Social Security Numbers of Borrowers, Co-Borrowers, Key Members, and Lender Identification Numbers, debt payment information, client names, lender names, addresses, and business financial data. **MFIS, MINC:** Information included contains social security numbers of borrowers, management agents, key members, and tenant social security numbers, debt payment information, customer names, tenant names, addresses, and business financial data.
3. Accuracy, Timeliness, and Reliability	
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	Data transmitted in ASCII File format through Gentran product must meet file format specifications and then each transaction is evaluated to meet business rules and USDA Regulations. Any transactions outside the expected values must be accepted by servicing

	personnel.
3b. How will data be checked for completeness?	1. The applications capability to establish access control lists (ACL) or registers is by based upon the basic security setup of the operating system. 2. Application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties via access given to user Ids limited to what is needed to perform their job. 3. The controls used to detect unauthorized transaction attempts are security logs/audit trails. 4. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access. 5. Warning banners are used to warn and inform users who sign on to the system that this is a secure and private network. Warning banners are in compliance with USDA guidelines.
3c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).	**AMAS:** Yes. The IDMS DBMS backup procedures on the AMAS database are established by the National Information Technology Center (NITC) for data restoration events. The data is backed-up nightly. Servicing Office personnel and the Deputy Chief Financial Officer (DCFO) staff verify data correctness via reports available within the AMAS application. **MFIS:** Yes. Oracle DBMS and Archive Procedures on the database are established by the St. Louis Web Farm for data restoration events. Servicing Office personnel and Management agents via reports available within the MFIS application verify data correctness. **MINC:** This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application. See the MFIS response for a description of the data displayed and or collected.
3d. Are the data elements described in detail and documented? If yes, what is the name of the document?	**AMAS:** IDMS schema Record Description reports are produced from the Data Dictionary that provide data element descriptions. **MFIS:** Encyclopedia Reports as generated by the Advantage Gen Central Encyclopedia. **MINC:** This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application. See the MFIS

	response for a description of the data displayed and or collected.

D. ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	**AMAS:** Yes. The data attributes provide loan processing information. **MFIS, MINC:** Yes. The data attributes provide Project servicing information.
2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	**AMAS:** Yes. The system generates a variety of daily, weekly, monthly, quarterly and yearly reports. This instrumental in the systems ability to provide up to date information on the loans portfolio. **MFIS:** Yes. The system generates a project worksheet. This instrument calculates the overage, RA and final payment for all projects on a monthly basis. **MINC:** This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application. See the MFIS response for a description of the data displayed and or collected.
3. Will the new data be placed in the individual's record (customer or employee)?	**AMAS:** No. The system is hierarchal by design and any individuals information is within this design and must be obtained by 'walking the data base' to gather information. **MFIS:** Yes. The systems stores a monthly record of the payment attributes. **MINC:** This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application. See the MFIS response for a description of the data displayed and or collected.
4. Can the system make determinations about customers or employees that would not be possible without the new data?	**AMAS:** No. It is the system's job to assemble loan detail information. **MFIS:** No. It is the system's job to assemble household and project detail information to determine monthly payments. **MINC:** This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application. See the MFIS response for a description of the data displayed and or collected.
5. How will the new data be verified for	**AMAS:** The data is reviewed by area specialists. **MFIS:** The data is reviewed by area specialists and

relevance and accuracy?	transferred to the project management agents. These management agents verify the data against their own records and approve the final payment details. **MINC:** The MFIS payment data is transferred to the project management agents via MINC. These management agents verify the data against their own records and approve the final payment details.
6. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	1. The applications capability to establish access control lists (ACL) or registers is based upon the basic security setup of the operating system. This system follows the USDA eAuthentication regulations. 2. Application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties via access given to user Ids limited to what is needed to perform their job. 3. The controls used to detect unauthorized transaction attempts are security logs/audit trails 4. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access. 5. Warning banners are used to warn and inform users who sign on to the system that this is a secure and private network. Warning banners are in compliance with USDA guidelines.
7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	Yes. The controls in 6 still apply.
8. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	**AMAS:** Data is retrieved by AMAS authorized users through login ID's using ACF2 IDs that are Management Agents/Service Bureaus Vendor Software on the NITC mainframe. It can be retrieved using an individual's Social Security Number. **MFIS:** Data is retrieved by MFIS authorized users using Level 2 eAuthentication user ID's that are cross-referenced with ACF2 login IDs that are verified on the NITC Mainframe. Access is restricted down to the state/servicing office level. With proper access, authorized users can retrieve data with by personal identifier. **MINC:** Data is retrieved by MINC authorized users

	through Level 2 login IDs that are verified within eAuthentication Security. Access is restricted down to management agent level. With proper access, authorized users can retrieve data with by personal identifier.
9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?	**AMAS:** Borrower Reports can be produced on individuals. Reports are used to perform daily functions and routine servicing of project within the RD portfolio. Servicing offices, State Offices, DCFO and National office have ability to review reports within their authorized areas. **MFIS:** Quick Check, Tenant History, Tenant Household, Management Agent Reports and Borrower Reports, Project worksheet. Servicing offices, State Offices and National office have ability to submit reports for project within their authorized areas. Reports are used to perform daily functions and routine servicing of project within the RD portfolio. **MINC:** The only reports available through MINC are the project worksheets and a list of transactions submitted by the user that is logged on to the application.
10. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses and how individuals can grant consent.)	None. Data required when obtaining project loans or rental assistance for a supported project.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS

1. If the system is operated in more than one site, how will consistent use of the system and data will be maintained in all sites?	**AMAS:** The system is hosted on a mainframe computer. Access is through user terminals, which are on the system. **MFIS, MINC:** The entire system is hosted in the STL web farm. Access is through user terminals, which are in the web farm.
2. What are the retention periods of data in this system?	**AMAS:** The system stores 3 years of history data online. Remaining history is kept on archived tapes and has infinite retention. **MFIS:** The system stores 3 years (or last 3 items) for

	annual data. Non-annual data has infinite retention. **MINC:** No. This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application.
3. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	**AMAS:** Once data is no longer needed, it is properly destroyed. Methods such as overwriting the entire media, degausses, and disk formatting are used, but strict attention is paid to whatever process is selected to ensure that all unneeded data is completely destroyed. Papers and other soft materials, such as microfiche and floppy disks, are shredded. **MFIS:** Annual data is shipped to the data warehouse via files produced on a monthly basis. Procedures are in place to assure that once data is no longer needed, it is properly destroyed. Methods such as overwriting the entire media, de-gaussers, and disk formatting are used, but strict attention is paid to whatever process is selected to ensure that all unneeded data is completely destroyed. Papers and other soft materials, such as microfiche and floppy disks, are shredded. **MINC:** No. This system is a display and collection system for the data held in MFIS. It does not store or maintain any data unique to the application.
4. Is the system using technologies in ways that the USDA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?	**AMAS:** No. **MFIS, MINC:** To avoid costly retrofitting of safeguards, sensitivity was afforded importance early in the life cycle. The needs for information protection were established during the initiation, development, and operation phases, and will be afforded appropriate review when termination occurs. To ensure that adequate safeguards, alternatives, and rules are in place and implemented this system is reevaluated periodically.
5. How does the use of this technology affect public/employee privacy?	**AMAS:** To avoid costly retrofitting of safeguards, sensitivity was afforded importance early in the life cycle. The needs for information protection were established during the initiation, development, and operation phases, and will be afforded appropriate review when termination occurs. To ensure that adequate safeguards, alternatives, and rules are in place and implemented this system is reevaluated periodically. **MFIS, MINC:** NONE

6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	**AMAS:** The system records an audit trail of who changes what data. This is used to identify how and when data changes were made that warrant explanation. **MFIS:** The system records an audit trail of who changes what data. This is used to identify how and when data changes were made that warrant explanation. **MINC:** The system records an audit trail of who changes what data. This is used to identify how and when data changes were made that warrant explanation.
7. What kinds of information are collected as a function of the monitoring of individuals?	**AMAS:** Project Data, Obligation Data, Check Data, Loan Data, Payment Data, History Data **MFIS, MINC:** Tenant Data: Member SSN, Birthday, Ethnicity, Race, Dependants information, annual income, medical costs, child care costs, total assets.
8. What controls will be used to prevent unauthorized monitoring?	**AMAS:** Audit Trails. **MFIS, MINC:** Firewall protection to the data servers and secure transfer protocol for web communications.
9. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	USDA / RD-SOR-1: Applicant, Borrower, Grantee, or Tenant File
10. If the system is being modified, will the SOR require amendment or revision? Explain.	**AMAS:** A change control process is in place whereby all changes to application software are tested and user approved prior to being installed into production. Changes to the applications are controlled by specific written requests for automation. Test results are kept until the turnover release warranty is expired and used as reference if necessary. Emergency fixes are handled in the same way as more extensive fixes except that they take priority over all other activity. There are no "hot keys" activated to facilitate the correction of data. **MFIS, MINC:** A change control process is in place whereby all changes to application software are tested and user approved prior to being installed into production. Changes to the applications are controlled by specific written requests for automation. Test results are kept until the turnover release warranty is expired and used as reference if necessary. Emergency fixes are handled in the same way as more extensive fixes except that they take priority over all

	other activity. There are no "hot keys" activated to facilitate the correction of data. Rural Development's SDLC and CM process requires the ISSS to review system changes for security documentation updates and re-accreditation decisions impact to ensure that the system SORN is revised as needed.

F. ACCESS TO THE DATA

1. Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, tribes, other)?	**AMAS:** USDA RD AMAS system users and managers. **MFIS:** USDA RD MFIS system users and managers, MFIS Systems Administrators, MFIS Trusted Management Agents. **MINC:** MFH External Trusted Partners or Management Agents.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	**AMAS, MFIS, MINC:** Desk Procedures document the process for establishing, activating, and modifying IDs. This process is defined by System Owners. System Owners define Groups and account types. System Point of Contact assigns group membership and determines Need-to-know validation. The POC is responsible for verifying user identification; the User Access Management Team (UAMT) relies on a POC supplying the correct userid and password to Logbook to identify themselves. Log Book tickets are the tool used to track authorized requests by approving Point of Contact (POC) Currently RD reviews reports from HR on a Bi-weekly basis. The organization employs automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are not used or authorized. Guest and Anonymous accounts are not managed by ISS UAM Team. POCs (empowered by RD IT managers) are responsible for notifying UAMT if access or roles need to be modified and periodically reviewing and certifying established access.

3. Will users have access to all data on the system or will the user's access be restricted? Explain.	No, users do not have access to ALL DATA on the system. Privileges granted are based on job functions and area of authority (e.g. State office user with authority for their state only, Management Agent versus a Management Agent User).
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	1. The applications capability to establish access control lists (ACL) or registers is based upon the basic security setup of the operating system. 2. Application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties via access given to user Ids limited to what is needed to perform their job. 3. The controls used to detect unauthorized transaction attempts are security logs/audit trails. 4. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access. 5. Warning banners are used to warn and inform users who sign on to the system that this is a secure and private network. Warning banners are in compliance with USDA guidelines.
5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, are Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?	Yes. All MFM contracts contain the appropriate Privacy Act clauses.
6. Do other systems share data or have access to data in this system? If yes, explain.	**AMAS:** The system utilizes input from PLAS and supplies input to PLAS through files during certain update cycles of the respective databases. The push to PLAS includes a FAADS data file which is merged with PLAS data and forwarded to the National Finance Center (NFC). The push to PLAS also includes General Ledger data that is merged with other data at PLAS. The system also supplies a file to the RD data warehouse. **MFIS:** MFIS is not connected to any external systems. The system utilizes input from the AMAS system and supplies input to the AMAS system through files during certain update cycles of the respective databases. The system supplies a file to the RD data warehouse.

	MINC: No. Data may be sent through MINC to the MFIS system but Data is not shared from MINC to vendor software.
7. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface?	Glen Boeckmann Glennon.boeckmann@stl.usda.gov 314-335-8598
8. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	**AMAS:** Farm Service Agency (PLAS) **MFIS, MINC:** No.
9. How will the data be used by the agency?	**AMAS:** To create and process loan applications with USDA and trusted Management Agents. **MFIS, MINC:** To create and process Project servicing activities with USDA and trusted Management Agents.
10. Who is responsible for assuring proper use of the data?	Glen Boeckmann Glennon.boeckmann@stl.usda.gov 314-335-8598

APPENDIX A

DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the United States Department of Agriculture to the public and are the responsibility of all USDA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the USDA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of USDA data systems, processes and facilities.

All USDA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the USDA, the USDA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.

Principle 4:	Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.
Principle 5:	Personally, identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 6:	Personally, identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.
Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the USDA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any USDA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.
Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the USDA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

APPENDIX B

POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The USDA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the USDA recognizes that compliance with legal requirements alone is not enough. The USDA also recognizes its social responsibility, which is implicit in the ethical relationship between the USDA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the USDA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the USDA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The USDA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. USDA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the USDA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the USDA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the USDA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.