

USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: USDA Rural Development

System Name: Multi-Family Management

System Type: **Major Application**
 General Support System
 Non-major Application

System Categorization (per FIPS 199): **High**
 Moderate
 Low

Description of the System:

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 Kansas City Web Farm.

Who owns this system?

Glen Boeckmann
Chief, Management Services Technologies Branch
USDA Rural Development
4300 Goodfellow Blvd.
St. Louis, MO 63120-1703
glennon.boeckmann@stl.usda.gov
314-457-4945

Who is the security contact for this system?

Eugene Texter
USDA Rural Development
Building 105, FC-44
4300 Goodfellow Boulevard
St. Louis, MO 63120
eugene.texter@stl.usda.gov
314-457-4778

Brenda Dinges
USDA Rural Development
Building 105, FC-44
4300 Goodfellow Boulevard
St. Louis, MO 63120
brenda.dinges@stl.usda.gov
314-457-4772

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

Who completed this document?

Glen Boeckmann
 Chief, Management Services Technologies Branch
 USDA Rural Development
 4300 Goodfellow Blvd.
 St. Louis, MO 63120-1703
 glennon.boeckmann@stl.usda.gov
 314-457-4945

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

QUESTION 1	Citizens	Employees
Does the system contain any of the following type of data as it relates to individual:		
Name	Yes	Yes
Social Security Number	Yes	No
Telephone Number	Yes	No
Email address	Yes	Yes
Street address	Yes	No
Financial data (i.e. account numbers, tax ids, etc)	Yes	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.?	Yes	No
NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code ¹		
Are social security numbers embedded in any field?	Yes	No
Is any portion of a social security numbers used?	Yes	No
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	No	No

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



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.

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

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.

DATA COLLECTION

3. Generally describe the data to be used 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. Voucher recipient name, Voucher payment borrower name, Monthly voucher amount.

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.

4. Is the collection of the data both relevant and necessary to the purpose for which the system is designed? In other words, the data is absolutely needed and has significant bearing on the system's purpose.

- Yes
 No. If NO, go to question 5

4.1. Explain.

AMAS: Yes. The data attributes provide loan processing and voucher processing information.

MFIS, MINC: Yes. The data attributes provide Project servicing information.

5. Sources of the data in the system.

5.1. What data is being collected from citizens and/or employees?

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. Voucher recipient name, Voucher payment borrower name, Monthly voucher amount.

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.

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

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

AMAS: Rural Development field office personnel collect the Loan Obligation information from prospective Borrowers/Applicants.

MFIS: 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: None

5.3. What government agencies (state, county, city, local, etc.) are providing data for use in the system?

AMAS: None

MFIS: None

MINC: NONE

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

AMAS: NONE

MFIS, MINC: Data transmitted in ASCII File format through Gentrans product from Management Agents/Service Bureaus Vendor Software.

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

- Yes
 No. If NO, go to question 7

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

- a. The applications capability to establish access control lists (ACL) or registers is based upon the basic security setup of the operating system.
- b. 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 is limited to what is needed to perform their job.
- c. The controls used to detect unauthorized transaction attempts are security logs/audit trails.
- d. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.
- e. 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.

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

Same as Above.

FOR OFFICIAL USE ONLY

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

- a. 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.
- b. Management Agents validate tenant data prior to approval of project worksheets.

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?

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).

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

- Yes
- No. If NO, go to question 9

8.1. What are the other purposes?

AMAS: The system generates a variety of daily, weekly, monthly, quarterly and yearly reports. This is instrumental in the systems ability to provide up to date information on the loans portfolio.

MFIS: 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.

9. Is the use of the data both relevant and necessary to the purpose for which the system is being used? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system’s purpose.

- Yes
- No. If NO, go to question 10

9.1. Explain.

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

AMAS: Yes. The data attributes provide loan processing information.

MFIS, MINC: Yes. The data attributes provide Project servicing information.

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.)?

Yes
 No. If NO, go to question 11

- 10.1. Will the new data be placed in the individual's record (citizen 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.

- 10.2. Can the system make determinations about citizens 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.

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

AMAS: The data is reviewed by area specialists.

MFIS: The data is reviewed by area specialists and 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.

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?

Same as the principle purpose (see # 7)

12. Will the data be used for any other purpose (other than indicated in question 11)?

Yes

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

No. If NO, go to question 13

12.1. What are the other purposes?

AMAS: The system generates a variety of daily, weekly, monthly, quarterly and yearly reports. This is instrumental in the systems ability to provide up to date information on the loans portfolio.

MFIS: 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.

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
 No. If NO, go to question 14

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

NIST 800-53A controls for the MFM system are discussed in detail in the System Security Plan.

Also:

- a. 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.
- b. 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.
- c. The controls used to detect unauthorized transaction attempts are security logs/audit trails
- d. Users are required to have password-protected screensavers on their PC's to prevent unauthorized access.
- e. 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.

14. Are processes being consolidated?

Yes
 No. If NO, go to question 15

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

See 13, 13.1 (Same as above)

FOR OFFICIAL USE ONLY

DATA RETENTION

15. Is the data periodically purged from the system?

- Yes – See below
- No

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

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.

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

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.

15.3. Where are these procedures documented?

AMAS: NITC controls cleaning of archival tapes and materials

MFIS: The Data Warehouse organization controls the cleaning and disposal of all data warehouse material no longer needed. Procedures for purging of data in MFIS is documented in the online help document MFIS Batch Processes.

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 purging of data.

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?

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.

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

- Yes – All data in use is necessary.
 No

DATA SHARING

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

- Yes - **AMAS:** Farm Service Agency (PLAS)
 Yes - **MFIS:** US Bank and FEMA
MINC: No.

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

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: 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. FEMA data contains no PII information and is used for determining vacancy information. US Bank data indicate the projects that need additional attention before processing monthly payments

MINC: Data may be sent through MINC to the MFIS system but Data is not shared from MINC to vendor software.

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

The system owner

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

- Yes
 No. If NO, go to question 20

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?

USDA PRIVACY IMPACT ASSESSMENT FORM

All external connections require an Interconnection Service Agreement.

19.2. Where are those documents located?

MFM (AMAS) to PLAS ISA is loaded in CSAM. A MOU to FEMA and an ISA to US BANK are being drafted.

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

- Yes
 No

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

AMAS: The system is hosted on a mainframe computer in NITC. Access is through user terminals, which are on the system.

MFIS, MINC: The entire system is hosted at Site A. Access is through user terminals, which are in the Kansas City Web Farm.

DATA ACCESS

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

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.

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

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.

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

- Yes

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

No. If NO, go to question 23

22.2. Where are criteria, procedures, controls, and responsibilities regarding user access documented?

See # 22

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

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).

Are procedures in place to detect or deter browsing??

Yes– See 13.1
 No

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

Yes– See 13.1
 No

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

Yes – See 13.1
 No

CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the citizens and employees affected by the interface (i.e. office, person, departmental position, etc.)?

The System/Application Owner

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

Citizens and employees may contact the Freedom of Information Officer:

Dorothy Hinden
Freedom of Information Officer
Rural Development, USDA
7th Floor, Reporter’s Bldg.
Washington, DC 20250
Dorothy.Hinden@wdc.usda.gov
(202)692-0031

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?

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

Yes - If YES, where is the breach notification policy located?

- U.S. Department of Agriculture Incident Notification Plan September 2007

- DM3505-001 USDA Computer Incident Response Procedures Manual.

- Computer Incident Response Standard Operating Procedures (CIRT)

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 citizens and employees of fundamental rules of fairness (those protections found in the Bill of Rights)?

Yes

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 citizens and employees?

DM 3515-002, section e states:

To fulfill the commitment of the USDA to protect customer and employee data, several issues must be addressed with respect to privacy:

- 1 The use of information must be controlled; and
- 2 Information may be used only for a necessary and lawful purpose.

Where Public Affairs systems of records are involved:

- 1 Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them;
- 2 Information collected for a particular purpose should not be used for another purpose without the subject's consent unless such other uses are specifically authorized or mandated by law; and
- 3 Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

Also, P.L. 95-454, the Civil Service Reform Act of 1978 which is enforced by The U.S. Equal Employment Opportunity Commission (EEOC) ensures the equitable treatment of the employees.

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

Yes

No. See Above.

SYSTEM OF RECORD

FOR OFFICIAL USE ONLY

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
 No

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

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.

- 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)

USDA / RD-SOR-1: Applicant, Borrower, Grantee, or Tenant File

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

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.

TECHNOLOGY

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

AMAS: No.

USDA PRIVACY IMPACT ASSESSMENT FORM

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.

32.1. How does the use of this technology affect citizens and employees 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

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

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

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 EGovernment Act of 2002.

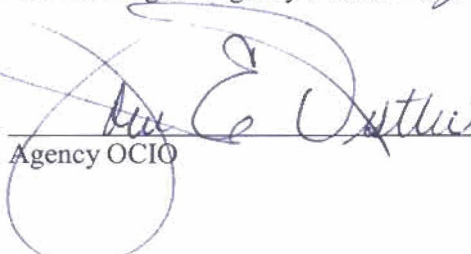
We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.


System Manager/Owner

6-12-2008
Date


Brenda Dinges - Agency's Chief FOIA Officer

6/30/08
Date


Agency OCIO

6/17/2008
Date

FOR OFFICIAL USE ONLY