Privacy Impact Assessment (PIA)

Electronic Debt and Loan Restructuring System (eDALR$)

Revision: Final
Privacy Impact Assessment for eDALR$
## Table of Contents

1 PURPOSE OF DOCUMENT .............................................................. 1

2 APPLICABILITY ........................................................................... 2
  2.1 Applicability of System .......................................................... 2
  2.2 System Overview ................................................................. 2
  2.3 System Categorization ......................................................... 2
  2.4 Responsible Organization .................................................. 2
  2.5 Information Contacts ......................................................... 3
  2.6 Assignment of Security Responsibility ............................... 4
  2.7 Who Completed this Assessment? ...................................... 5

3 USDA PRIVACY IMPACT ASSESSMENT .................................... 6
  3.1 Does the System Contain Information About Individuals in an Identifiable Form? ........................................... 6
    3.1.1 Data Collection ............................................................. 8
    3.1.2 Data Use .................................................................... 9
    3.1.3 Data Retention .......................................................... 10
    3.1.4 Data Sharing ............................................................. 11
    3.1.5 Data Access ............................................................... 11
    3.1.6 Customer Protection .................................................. 12
    3.1.7 System Of Record ...................................................... 13
    3.1.8 Technology ................................................................. 14

4 PRIVACY IMPACT ASSESSMENT AUTHORIZATION MEMORANDUM ......................................................... 1
1 Purpose of Document

USDA DM 3515-002 states: "Agencies are responsible for initiating the PIA in the early stages of the development of a system and to ensure that the PIA is completed as part of the required System Life Cycle (SLC) reviews. Systems include data from applications housed on mainframes, personal computers, and applications developed for the Web and agency databases. Privacy must be considered when requirements are being analyzed and decisions are being made about data usage and system design. This applies to all of the development methodologies and system life cycles used in USDA.

Both the system owners and system developers must work together to complete the PIA. System owners must address what data are used, how the data are used, and who will use the data. System owners also need to address the privacy implications that result from the use of new technologies (e.g., caller identification). The system developers must address whether the implementation of the owner's requirements presents any threats to privacy.

The Privacy Impact Assessment (PIA) document contains information on how the Electronic Debt and Loan Restructuring System (eDALRS) affects the privacy of its users and the information stored within. This assessment is in accordance with NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems."
2 Applicability

2.1 Applicability of System

The information in this document is applicable to the Electronic Debt Loan & Restructuring System (eDALR$).

2.2 System Overview

The Electronic Debt and Loan Restructuring System (eDALR$) is a web-based support tool that assists the United States Department of Agriculture (USDA), Farm Service Agency (FSA) Authorized Agency Official in determining and evaluating the effects of primary loan servicing options in accordance with FSA Handbook 5-FLP. In computing a debt restructuring plan, eDALR$ considers all primary loan servicing programs to maximize the borrower's ability to repay debt while remaining solvent, and avoid financial loss to the Government.

eDALR$ assists field office employees in restructuring customer debt from loans originating from the USDA farm loan programs. When a borrower is in a position of financial distress and are investigating the option of restructuring their existing USDA loans, they begin the restructuring process by first meeting with a county field office servicing official. The servicing official begins the process by querying USDA financial systems that hold information for the customer's debt obligations. The official either manually enters or imports the debt information into eDALR$ where calculations are performed according to the requirements in 7 CFR Part 1951. The results of the program present options to the borrower for restructure and or reamortization of the debt over a specified repayment period, deferral of repayment of debt for an additional period, consolidation of debts into a new loan, or a commitment by the USDA to write-down portions of the debt to reflect current conditions, values, and ability to pay. Proposal scenarios that are output from eDALR$ are generated in the form of an electronic document that are printed and handed to or mailed to the borrower for an acceptance decision concerning the restructure offer. The generated proposal documents are passed to a document management system for storage. The involvement of the eDALR$ application ends at this point.

2.3 System Categorization

By following the guidance set forth in NIST SP 800-60 and FIPS PUB 199 taking into account the information types and other factors for this system, the Security Categorization for this system has been determined to be Moderate. Therefore, Risk Assessments and Security Testing and Evaluation (ST&E) will be performed following the Moderate baseline set forth in NIST SP 800-53 Annex 2.

2.4 Responsible Organization

United States Department of Agriculture (USDA)
Farm Service Agency (FSA)
1400 Independence Avenue SW
Washington, D.C. 20250

This system is maintained by:
Farm Service Agency
USDA/FSA/ITS/FCAO/FLPDG
6501 Beacon Dr.
The system hardware is located at:
USDA/Farm Service Agency
National Information Technology Center (NITC)
8930 Ward Parkway
Kansas City, MO 64114

2.5 Information Contacts

- Certification Agent
  Sue E. Bussells
  FSA Chief Information Officer (Acting)
  Director, Information Technology Services Division (ITSD) (Acting)
  FSA/DAM/ITSD
  U.S. Department of Agriculture
  Farm Service Agency
  1400 Independence Avenue SW
  Washington D.C. 20250
  (202) 720-5320
  sue.bussells@wdc.usda.gov

- Authorizing Official (Designated Approval Authority - DAA)
  Carolyn Cooksie
  Deputy Administrator Farm Loan Programs/FSA
  USDA/FSA/DAFLP
  U.S. Department of Agriculture
  Farm Service Agency
  1400 Independence Avenue SW
  Washington D.C. 20250
  (202) 720-7597
  carolyn.cooksie@wdc.usda.gov

- User Representative
  Sharilyn Hashimoto
  USDA/FSA/DAFLP/LSPMD/DLSB
  U.S. Department of Agriculture
  Farm Service Agency
  1250 Maryland Ave. SW / Suite 500
  Washington D.C. 20024
  (202) 720-2743
  sharilyn.hashimoto@wdc.usda.gov

- Information Owner
  Veldon Hall
  USDA/FSA/DAFLP/LSPMD
  U.S. Department of Agriculture
2.6 Assignment of Security Responsibility

- Privacy Act Officer
  Karen Malkin
  Chief Privacy Act Officer
  USDA/FSA/OA
  U.S. Department of Agriculture
  Farm Service Agency
  1400 Independence Avenue SW
  Washington, D.C. 20250
  (202) 690-2203
  karen.malkin@wdc.usda.gov

- Freedom of Information Act (FOIA) Coordinator
  Thomas B. Hofeller, Acting
  Associate Administrator for Operations and Management
  USDA/FSA/OA
  U.S. Department of Agriculture
  Farm Service Agency
  1400 Independence Avenue SW
  Washington, D.C. 20250
  (202) 690-0153
  tom.hofeller@wdc.usda.gov

- Information System Security Manager
  Brian Davies
  Information System Security Program Manager (ISSPM)
  FSA/DAM/ITSD/OTC/ISO
  U.S. Department of Agriculture
  Farm Service Agency
2.7 Who Completed this Assessment?

Kathy Serrone
Computer Specialist, FCAO/FLPDG
6501 Beacon Dr.
Kansas City, MO 64133
816-926-6380
kathy.serrone@kcc.usda.gov
3 USDA Privacy Impact Assessment

3.1 Does the System Contain Information About Individuals in an Identifiable Form?

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

<table>
<thead>
<tr>
<th>QUESTION 1</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>☒</td>
<td></td>
</tr>
<tr>
<td>Social Security Number</td>
<td>☒</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td></td>
<td>☒</td>
</tr>
<tr>
<td>Email address</td>
<td></td>
<td>☒</td>
</tr>
<tr>
<td>Street address</td>
<td></td>
<td>☒</td>
</tr>
<tr>
<td>Financial data</td>
<td>☒</td>
<td></td>
</tr>
<tr>
<td>Health data</td>
<td></td>
<td>☒</td>
</tr>
<tr>
<td>Biometric data</td>
<td></td>
<td>☒</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QUESTION 2</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.?</td>
<td>☒</td>
<td></td>
</tr>
</tbody>
</table>

NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code

Are social security numbers embedded in any field? | ☒ | ☒ | ☒ |
| Is any portion of a social security number used? | ☒ | ☒ | |
| Are social security numbers extracted from any other source (i.e. system, paper, etc.)? | ☒ | ☒ | |

---

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.
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-I1, 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.
3.1.1 Data Collection

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

The data consists of borrower information with regard to loan(s), financials, and security property.

2. 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
☐ No

3. Sources of the data in the system.

3.1. What data is being collected from the customer?

Borrower information with regard to loan(s), financials, and security property.

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

Farm Service Agency

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

N/A

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

N/A

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

☐ Yes
☒ No. If NO, go to section 3.1.2, question 1.

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

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

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

1. 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?

   To assist in determining the most optimal servicing solutions applicable and available.

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

   [ ] Yes
   [x] No. If NO, go to question 3 (below).

2.1 What are the other purposes?

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.

   [x] Yes
   [ ] No

4. 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
   [x] No. If NO, go to question 5 (below).

4.1 Will the new data be placed in the individual’s record (customer or employee)?

   [ ] Yes
   [ ] No

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

   [ ] Yes
   [ ] No

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

5. 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 intended routine use is to assist FSA personnel in determining the most optimal servicing solutions applicable and available to the individual. The information is not collected for use in a routine outside of the application.
6. Will the data be used for any other uses (routine or otherwise)?

☐ Yes
☒ No. If NO, go to question 7 (below).

6.1 What are the other uses?

7. 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 8 (below).

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

Users must be authorized by management before access is given to the application. Users must be authenticated to the system first through eAuth Level 2 access and then have been assigned the appropriate roles and locality to the application via the Extensible Authentication System (EAS) before users can access online data relevant to eDALR$.

8. Are processes being consolidated?

☐ Yes
☒ No. If NO, go to section 3.1.3, question 1.

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

3.1.3 Data Retention

1. Is the data periodically purged from the system?

☐ Yes
☒ No. If NO, go to question 2 (below).

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

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

1.3 Where are these procedures documented?
2. 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?

Due to litigation requirements, data is required to be kept indefinitely with no expiration.

3. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?
   - Yes
   - No

3.1.4 Data Sharing

1. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?
   - Yes
   - No. If NO, go to question 2 (below)

1.1 How will the data be used by the other agency?

1.2 Who is responsible for assuring the other agency properly uses the data?

2. Is the data transmitted to another agency or an independent site?
   - Yes
   - No. If NO, go to question 3 (below)

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

3. Is the system operated in more than one site?
   - Yes
   - No. If NO, go to section 3.1.5, question 1.

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

3.1.5 Data Access

1. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?
   - Field office users, managers, system administrators.
2. How will user access to the data be determined?

Specific EAS roles must be assigned to the user's eAuth ID.

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

☐ Yes
☐ No

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

Specific EAS roles and locality codes are assigned to the users to allow them restricted access to the information for those individuals that reside in the users' assigned service locations.

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

☐ Yes
☐ No

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

☐ Yes
☐ No

3.1.6 Customer Protection

1. 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.)?

The protection of privacy of the customer's information is the responsibility of each person that has been given access to retrieve or view information from this system, whether directly retrieved by individuals with access to the system or by those that may handle any paper documents generated by the application. All users are made aware of their responsibilities through annual privacy and security awareness training.

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

Contact the FSA Privacy Officer.

Karen Malkin
Chief Privacy Act Officer
USDA/FSA/OA
U.S. Department of Agriculture
Farm Service Agency
1400 Independence Avenue SW
Washington, D.C. 20250

Contact the FSA Privacy Officer.

Karen Malkin
Chief Privacy Act Officer
USDA/FSA/OA
U.S. Department of Agriculture
Farm Service Agency
1400 Independence Avenue SW
Washington, D.C. 20250
3. 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 4 (below).
☐ No

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

4. 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)?

☐ Yes
☒ No. If NO, go to question 5 (below).

4.1 Explain how this will be mitigated.

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

eDALR$ was developed for just that purpose to ensure that all available servicing options were reviewed and if applicable, offered to our customers.

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

☐ Yes
☐ No. If NO, go to section 3.1.7, question 1.

6.1 Explain

3.1.7 System Of Record

1. 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. If NO, go to section 3.1.8, question 1.

1.1 How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?
Data may be retrieved through searching by Name, Business Name, or social security/tax identification number.

1.2 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/FSA-2 Farm Records File/Automated
USDA/FSA-14 Applicant/Borrower

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

3.1.8 Technology

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

☐ Yes
☒ No. If NO, the Questionnaire is Complete.

1.1 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
4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Electronic Debt and Loan Restructuring System (eDALR$)

(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.

Arthur V. Hall
Information Owner

Date: 8-22-08

Steven L. Sanders
Agency CIO

Date

Karen Malkin
Chief Privacy Act Officer

Date
4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Electronic Debt and Loan Restructuring System (eDALR$)

(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.

Arthur V. Hall
Information Owner

Sue E. Bussells
Agency CIO (Acting)

Date: September 4, 2008
4 Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Electronic Debt and Loan Restructuring System (eDALRS)

(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.

___________________________  _______________________
Veldon Hall  
Information Owner  

___________________________  _______________________
Sue Bussells  
Agency CIO (Acting)  

___________________________  9/8/2008  
Brian Davies  
Information System Security Program Manager (ISSPM)