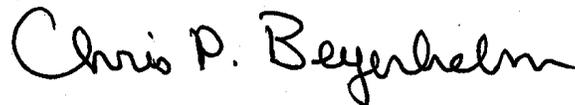


For: FSA Offices

Interim Policy for Safeguarding Privacy Act Protected Data

Approved by: Acting Deputy Administrator, Farm Loan Programs



1 Overview

A Background

All FSA employees have a significant responsibility to ensure that Privacy Act protected data entrusted to FSA is:

- secure
- not divulged to unauthorized personnel, lost, or stolen.

FSA’s commitment to fulfilling this responsibility has been communicated with the:

- issuance of Notices IRM-371, IRM-372, and IRM-378
- requirement to complete Privacy Act training as required by Notice IRM-373.

OMB recently asked Federal agencies to review their processes for collecting, storing, and controlling access to data. In response, FLP established a taskforce to review its overall policies regarding the gathering and protection of Privacy Act protected data provided by FLP applicants and borrowers.

For the short term, the taskforce is focusing its efforts on restricting access and ensuring the protection of Privacy Act protected data:

- included in reports and correspondence
- maintained:
 - in borrower case folders
 - FLP files established according to 25-AS, Exhibit 40.5
 - on CCE portable computers
 - on FSA information systems, such as PLAS, GLS, and FBP.

Disposal Date	Distribution
October 1, 2007	All FSA Offices; State Offices relay to County Offices

Notice FLP-447

1 Overview (Continued)

A Background (Continued)

For the long term, using a random, system-generated number instead of the borrower's SSN/Employer Identification Number (EIN) when establishing the case number was considered; however, significant implementation costs would be incurred. Therefore, the first 5 digits of SSN/EIN portion of the case number will be suppressed on system-generated reports, forms, and correspondence (except for IRS related and payment disbursement documents). The suppression of the first 5 digits of SSN/EIN will be implemented incrementally over the upcoming months, beginning with Report Code 540.

B Purpose

This notice provides interim guidance regarding Privacy Act protected data collected or maintained in the administration of FLP.

2 Interim Policies

A Definition of Privacy Act Protected Data

For purposes of this notice, Privacy Act protected data is defined as any data about an individual maintained by the Agency in a system of records that contains the individual's name identifying number, symbol, or other identifying particular assigned to the individual, and any of the following:

- SSN
- EIN
- date of birth
- home address
- financial information
- other items, collections, or groupings of information about an individual such as education (excluding training information for government employees), medical history, and criminal or employment history.

Notice FLP-447

2 Interim Policies (Continued)

B Reports

Copies of reports will be filed according to 25-AS, Exhibit 40.5.

Note: Refer to 25-AS, subparagraph 43 B and 3-INFO, paragraph 3 for information about safekeeping files that include sensitive documents.

C Correspondence

Internal or external correspondence generated by offices other than the St. Louis Farm Loan Operations Office (STFLOO), should **not** include the full SSN/EIN in the case number unless it is necessary for the recipient of the correspondence to take action, to properly identify the customer, or is legally required or advised.

Example: The full SSN or EIN is required for notice to potential purchasers under 7 CFR 1962.13.

D Borrower Case Folders and Other FLP Files

Before March 30, 2007, State and County Offices shall modify the labels on **all** active and closed:

- borrower case folders by either:
 - printing and attaching a new label with the with first five digits of the SSN/EIN in the case number replaced by X's

Example: If the borrower's full case number is 24-07-123456789, enter 24-07-XXXXX6789.

- using a marker to conceal the first five digits of the SSN/EIN in the case number

Note: 25-AS, subparagraph 82 D does not include "address" in the information to be included on the label for a borrower's case folder. If the borrower's address is listed on the label, it shall:

- not be included when the label is reprinted
- be concealed using a marker, if a new label is **not** printed.

2 **Interim Policies (Continued)**

D Borrower Case Folders and Other FLP Files (Continued)

- property acquisition folders by either:
 - printing and attaching a new label:
 - with the first 5 digits of the SSN/EIN in the former borrower's case number replaced by "X"s
 - without the property address
 - using a marker to conceal the first 5 digits of the SSN/EIN in the case number and the property address.

As provided by 25-AS, subparagraph 43 B, files containing Privacy Act protected data:

- need to be stored in locked file cabinets
- should **not** be left out on desks when leaving the office for a short time or at the end of the day.

E Delivery or Transfer of Borrower Case Folders

When a borrower case folder must be delivered to another location, the transfer shall be completed using any method of delivery authorized in 5-AS that provides for both the tracking and confirmation of delivery.

F Transmitting Privacy Act Protected Data

Effectively immediately, County, State, and National Offices, as well as STFLOO, shall only transmit data by FAX if the first 5 digits of SSN/EIN portion of the borrower's case number and other sensitive data can be concealed (without altering the original document).

Exception: The borrower's full case number may be included when the recipient of the document requires the full SSN/EIN to process a transaction or action, such as funding, Treasury requirements, etc.

Note: Refer to 6-IRM, paragraph 44 for additional guidance about using a FAX to transmit or receive data.

Privacy Act protected data may be transmitted:

- electronically across a USDA LAN
- over the Internet, by e-mail, CD, or floppy disk **only** if encrypted according to Notices IRM-372 and IRM-378.

Notice FLP-447

2 Interim Policies (Continued)

G Restrictions on Downloading and Storing Privacy Act Protected Data

All employees:

- shall follow the policies in Notice IRM-371 about downloading and storing Privacy Act protected data
- with CCE portable computers shall ensure files containing sensitive data are encrypted according to Notice IRM-378.

H FSA Information Systems

Employees are responsible for ensuring Privacy Act protected data and other sensitive information maintained in FSA information systems is safeguarded. As required by 6-IRM, subparagraph 56 B, employees shall:

- restrict access to FSA computer rooms and equipment to authorized users only
- ensure computer equipment in public areas is placed so that a customer cannot see the screen without permission
- ensure that workstations are locked, use a screen saver that is password protected, or shut down when unattended.

Supervisors will ensure the provisions of Notice IRM-382 are met when requesting employees be granted access privileges to electronic records systems.

I Contacts

The following table provides contacts if there are questions about this notice.

IF located in a...	THEN contact...
County Office	State Office.
State Office	State Offices shall contact: <ul style="list-style-type: none">• ITSD staff or help desk as provided in Notices IRM-371, IRM-272, and IRM-378 for IT related issues• Chris Beyerhelm at 202-720-7597 for FLP related issues.