UNITED STATES DEPARTMENT OF AGRICULTURE
Farm Service Agency
Washington, DC 20250

Notice IRM-398

For: FSA Employees and Contract Employees

FSA Computer Security Procedures

Approved by: Deputy Administrator, Management

1 Overview

A Background

FSA has several forms for granting access privileges to FSA IT systems.

In FY 2006, FSA had an independent audit review (per OMB Circular A-123) which determined that improvements could be made in FSA's security access request processes and procedures. FSA management and the Information Security Office (ISO) implemented the following:

- a of review current procedures and forms used by FSA for collecting, processing, and controlling information security access requests
- improvements to security access request procedures.

As part of the improvements to the access request procedures, in October 2006, FSA-13-A was released replacing all previous versions of FSA-13-A's, FSA-13-B's, FSA-13-D's, FSA-13-H's FSA-13-I's, KC-328's, and KC-330's.

B Purpose

This notice:

- provides new versions of FSA-13 and FSA-13-A; FSA-13-A changes include **not requiring SSN's**
- obsoletes Notice IRM-382

Disposal Date	Distribution
October 1, 2008	All FSA employees and contractors; State Offices relay to County Offices

1 Overview (Continued)

B Purpose (Continued)

- impacts **all** security access requests for **all** FSA information system users by employees and contractors

- provides procedures, FSA-13's, and FSA-13-A's for requesting new or modified user access to **any** USDA/FSA applications granted by or through ISO.

Note: FSA-13 (08-31-07) and FSA-13-A (09-17-07) are required for access requests. Both FSA-13's and FSA-13-A's are updated with this notice.

C User Compliance

Users **must** comply with procedures in this Notice, in addition to all other applicable Federal, USDA, FSA, OCIO, and ITS requirements. Included in this notice is the following guidance and instructions for requesting access privileges to FSA IT systems:

- FSA-13 (see Exhibit 1)

- a completed FSA-13-A displaying required entries (see Exhibit 2)

- instructions for completing FSA-13-A (see Exhibit 3)

- a chart showing FSA systems, system access requirements, and contacts for access issues (see Exhibit 4)

- a chart showing FSA roles, used in FSA-13-A, item 38 (see Exhibit 5).

Note: FSA-13 (08-31-07) and FSA-13-A (09-17-07) obsolete **all** previous versions of FSA-13 and FSA-13-A, and obsoletes FSA-13-G, FSA-13-H, FSA-13-I.

All new contractors and temporary and permanent County and Federal users needing computer access are required to submit FSA-13 and FSA-13-A **before** being given access to FSA computers and applications. Additionally, requests to modify, add, or delete accesses to FSA applications must be submitted using FSA-13-A.

Notes: For multi-agency applications where management has determined different internal procedures, users will follow procedures found in applications/systems handbooks such as 1-CM and Notice CM-560 for the Service Center Information Management System (SCIMS), and Notice CM-562 for Subsidiary, DCP Contracts, and the Farm Records Management System web-based applications.

SCIMS access is processed by FSA SCIMS Security Officers.

2 Responsibilities

A Supervisor/Contracting Officer's Technical Representative (COTR) Responsibilities

All managers, supervisors, and COTR's have a significant responsibility to ensure that:

- **existing procedures** outlined in the documentation of Multi-Agency Systems, such as 1-CM, Notice CM-560 for SCIMS, or applicable handbooks and Notice CM-562 for Subsidiary, DCP Contracts, and FRS web-based applications, are followed instead of the procedures outlined in this notice

- forms are filled out **completely** and returned to the appropriate office.

It is the responsibility of each supervisor/COTR who signs FSA-13-A (Exhibit 2), to determine who should be granted access **privileges** to information systems, and to:

- confirm that the individual has signed FSA-13

- complete and submit FSA-13-A to the Security Liaison Representative (SLR)/FSA Information Security Operation Support (ISOS)

- confirm that, if not already completed, a background check has been requested from Human Resources (according to 2-PM and 27-PM) to SLR/ISOS

- confirm that the individual has completed their **Computer Security Awareness Training**

  Note: Individuals will be provided Security Awareness Training by their supervisor/COTR **before** receiving a computer user ID. This training provides individuals with "Security Expectations and Rules of Behavior" and "Security Incident Response Guide for Users", but does **not** substitute for taking the full training course described in Notice IRM-388.

- submit FSA-13-A requesting **removal of access privileges when a user no longer needs access because of transfer, job change, resignation, retirement, termination, or any other separation from the supervisor's/COTR's organization or change in business need**; this request should be submitted **before** the access is no longer needed.

Note: If FSA-13-A is **not** submitted to SLR/ISOS, the user's access request will **not** be granted. If unneeded accounts or access privileges are discovered during an audit or review, the individual's 2nd line manager will be notified.

2 Responsibilities (Continued)

A Supervisor/Contracting Officer's Technical Representative (COTR) Responsibilities (Continued)

FSA-13-A's are:

- required when requesting creation, deletion, and modification to any FSA, NITC, NFC, ITS, and/or other agency's systems and/or applications available for access privileges by FSA employees, contract employees, and partners, except for SCIMS, DCP Contracts, Subsidiary, and FRS web-based applications

- submitted through SLR/ISOS.

If FSA-13-A's are **not** submitted to SLR/ISOS, access will **not** be granted.

B SLR Responsibilities

SLR's are responsible for the following:

- processing the parts of FSA-13-A's for which SLR has authority
- submitting FSA-13-A's, as appropriate, to ISOS for processing
- maintaining electronic and/or paper copies of FSA-13-A's
- contacting individuals and/or supervisors/COTR's upon completion
- reviewing quarterly, a sample of applications to which users have access privileges
- reviewing active ID's on FSA systems and applications.

C ISOS Responsibilities

ISOS is responsible for the following:

- processing the parts of FSA-13-A's to which ISO has authority

- submitting FSA-13-A's to the appropriate Agency or office for additional processing; such as NFC, NITC, ITS, etc.

- maintaining electronic and/or paper copies of FSA-13-A's

- contacting SLR's, individuals, and/or supervisors/COTR's upon completion

- reviewing quarterly a sample of applications to which users have access privileges

- reviewing active ID's on FSA systems and applications

- training/instructing SLR's, individuals, and/or supervisors/COTR's on proper access privileges request procedures.

2 Responsibilities (Continued)

D Users Responsibilities

It is the responsibility of each individual requesting access and to whom management grants the privilege to access an FSA information system to:

- read, sign, and submit FSA-13 to the user's manager
- complete and submit FSA-13-A to the user's manager

  Note: Users are **never** permitted to submit FSA-13-A's on their own behalf.

- confirm that a background check has been requested from HRD or their Administrative Officer
- confirm, to supervisor/COTR, that they have completed their Computer Security Training.

3 Procedures

A Large Offices Procedures

Large offices include the National Office; Kansas City, Missouri; St. Louis, Missouri; and APFO.

Supervisors/COTR's shall submit FSA-13-A's to ISOS for processing on the behalf of users.

Note: Users are **never** permitted to submit FSA-13-A's on their own behalf. Users **must** have a member of their management chain sign and submit FSA-13-A's to ISOS.

B Procedures for Service Center Offices

Service Center Offices include State Offices, County Offices, and District Offices.

The individual's local supervisor/COTR submits FSA-13-A to the designated SLR for the user's Service Center. SLR's submit FSA-13-A's to FSA's ISOS.

Note: Users are **never** permitted to submit FSA-13-A's on their own behalf. Users **must** have a member of their management chain sign and submit FSA-13-A's to ISOS.

4 Acceptable Request Format

A FSA-13-A (09-17-07)

FSA-13-A:

- is the **only** acceptable system access request format for privileges, except for SCIMS, DCP Contracts, Subsidiary, and FRS
- obsoletes **all** previous versions of FSA-13 and FSA-13-A
- obsoletes FSA-13-G, FSA-13-H, and FSA-13-I.

Completed FSA-13-A's can be submitted by FAX to 816-627-0687.

For more information on access privileges, contact the ITSD Information Security Office, ISOS, by:

- e-mail to **security@kcc.usda.gov**
- FAX to 816-627-0687.

Example of FSA-13

The following is an example FSA-13.

This form is available electronically.
FSA-13
(08-31-07)

U.S. DEPARTMENT OF AGRICULTURE
Farm Service Agency

FSA COMPUTER SECURITY AGREEMENT

An agreement between _____ and the USDA/Farm Service Agency (FSA).
(Print or Type Name)

1. PURPOSE. This document is meant to obtain an individual agreement to abide by security requirements and procedures needed to protect FSA and customer information resources. It is also intended to help raise security awareness and inform workers about security policies and procedures and to provide workers an opportunity for asking questions about these matters.

2. AUTHORITIES. National policy requirements regarding information systems are stated in the Federal Information Security Management Act (Title III of the E-Government Act of 2002); the Computer Fraud and Abuse Act (18 U.S.C. Sec. 1030 [1993]); Office of Management and Budget (OMB) Circular No. A-123, Management Accountability and Control; and OMB Circular A-130, Management of Federal Information Resources. These documents along with USDA security policies prescribe and set standards for establishing and maintaining a comprehensive information security program and use of information systems.

3. SCOPE. This agreement applies to FSA workers (both employees and contractors) who operate, maintain, and/or use Information Technology (IT) systems.

4. UNDERSTANDING AND AGREEMENTS. As a user of IT systems, I:

- Will protect FSA and customer systems in accordance with Federal, USDA, FSA and OCIO policies.
- Will use USDA and/or FSA computer systems (e.g., computers, systems, laptops, PEDs, networks, etc.) only for authorized purposes. If using the computer systems and networks for nonofficial purposes, I will do so within the bounds allowed by USDA policy, supervisor approval, and without interfering with official business.
- Will protect systems and all sensitive information from electronic or physical access by unauthorized personnel. I will protect computer equipment, media, telecommunications, and similar assets from theft, fraud, misuse, loss, unauthorized modification, and unauthorized denial of use. I will make every effort to avoid action/inaction that could jeopardize mission success, customer rights, individual privacy, or the reputation of the FSA.
- Understand that systems and other information resources, including electronic mail and Internet access, are primarily intended for official business and may be monitored. Although FSA policy permits limited personal use, I understand that my personal use must not interfere with official business and that I have no expectation of personal privacy when using these systems.
- Will not intentionally access, delete or alter files, operating systems or programs, except as specifically authorized for official business.
- Will not leave FSA computers in an operational state (e.g., "logged on") while unattended. I will either turn off the computer system, manually lock the screen, or set a time activated password-protected screen saver.
- Will abide by software copyright licenses and restrictions. I will not load any unapproved software (e.g., software from home, games, etc.) or install hardware or peripheral devices (e.g., external hard drives, docking stations, thumb drives, etc) on FSA systems without my supervisor's permission.
- Will not download file-sharing software (e.g., MP3 music, video files, etc.), peer-to-peer software (e.g., Kazaa, Napster, etc.), or games onto FSA systems or networks.

_____
(User Initials)

Example of FSA-13 (Continued)

- Acknowledge that I will receive user identifiers (user IDs) and passwords to authenticate my computer account. After receiving them, I will:
  - Immediately change the password.
  - Protect and not share or publicly post my password. If my password has been compromised, I will report the issue to my supervisor or security personnel.
  - Not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED) or other media unless approved by security personnel.
  - Be responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when logged on a system with that account.
  - Ensure my password is changed regularly or if compromised.
  - Ensure my password meets USDA complexity requirements.
- Will use anti-virus software in an effective way to prevent damage or disruption to FSA operations. I will scan all removable media (e.g., disks, CDs, thumb drives, etc.) for malicious software (e.g., viruses, worms, etc.) before using it on any government owned computer system or network.
- Will take appropriate steps to protect important data from loss (e.g., backups).
- Will not use Government owned computers, networks or IT services for purposes that violate ethical standards, including harassment, threats, sending or accessing sexually explicit material, racially or ethnically demeaning material, gambling, chain letters, for-profit activities, political activities, promotion or solicitation of activities prohibited by law, and so forth. If I use Government owned computer systems and networks, I will do so within the bounds allowed by USDA policy and supervisor approval and without interfering with official business.
- Will not try to disable or subvert ITS and FSA security controls or monitoring mechanisms.
- Will not attempt to break into any computer, whether Federal, USDA, or private, for which access is not authorized. Attempted break-ins may be authorized by my organization's Information System Security Program Manager (ISSPM) only for functions such as approved security tests, approved attempts to recover a system after a password is lost/forgotten, and similar functions.
- Will practice good housekeeping with all electronic equipment, including keeping food, beverages, or other contaminants away from computers and data storage media.
- Will report suspected/actual security incidents and other security concerns to my supervisor and my organization's ISSPM.
- Will stay abreast of security issues through education and awareness products distributed throughout USDA. I will attend at least one (1) security awareness session each year.
- Will not disclose sensitive data. In the course of performing work at FSA, I realize it may be necessary for me to have access to sensitive information, which includes:
  - Proprietary information – technical information or trade secrets, that is proprietary.
  - Privacy information – information protected under the provisions of the Privacy Act of 1974.
  - Privileged information – financial or commercial information that must be restricted from disclosure on the basis of Federal law or contractual agreement.
  - Government information – information or data stored, processed or handled in providing services under any FSA contract.

_____
(User Initials)

Example of FSA-13 (Continued)

FSA-13 (08-31-07) Page 3 of 3

I have read and understand the FSA Security Agreement on the use of government Information Technology (IT) systems. I understand that unauthorized or inappropriate use of government IT systems may result in the loss or limitation of my privilege. I also understand that I could face administrative action ranging from counseling to removal from the agency, as well as any criminal penalties or financial liability, depending on the severity of the misuse.

5. EFFECTIVE DATE. This agreement becomes effective when signed and dated. Refusal to sign may result in being denied use of any or all USDA information systems including e-mail and network access to the Internet.

NOTE: Refusal to sign does not relieve the individual of responsibility to abide by the standards set forth in this and related documents. (Supervisor/COR/COTR: If the worker refuses to sign, notate that fact on the signature line and retain this document.)

6. User's Signature	7. Telephone Number	8. Date
9. Person Signing Is *(Check One)*: ☐ Federal Employee	☐ Contractor	
10. Organization	11. If Contractor – Company Employed By	
12. Supervisor/COR/COTR Signature	13. Supervisor/COR/COTR Title	14. Date

USDA IS AN EQUAL OPPORTUNITY EMPLOYER

Example of FSA-13-A

The following is an example of a completed FSA-13-A.

This form is available electronically. See Page 3 for Completion Instructions.

FSA-13-A (09-17-07) U.S. DEPARTMENT OF AGRICULTURE Farm Service Agency

DATA SECURITY ACCESS AUTHORIZATION FORM

INSTRUCTIONS: Please complete a separate form for each employee or contractor.

1. Request Date:
2. Request Type: ☐ ADD ☐ MODIFY ☐ DELETE

3. Last Name
4. Full Legal Name *(Including middle and suffix)*
5. Full Organizational Acronym *(e.g. DAM/ITSD/OTC)*
6. Room/Cube No.
7. Office Phone No. *(Include Area Code)*
8. Office Fax No. *(Include Area Code)*
9. FSA User Email Address
10. Request Effective or Start Date:
11. Employee Type *(Check applicable box):* ☐ KC ☐ STL ☐ WDC ☐ ST/CO ☐ CONTRACTOR ☐ OTHER (Specify):
12. Temporary Access ☐ YES If "YES", Termination Date of Temporary Access:
13. Was "Background Investigation" performed, (or in process)? ☐ YES ☐ NO
14. Was "Security Awareness Training" completed? ☐ YES ☐ NO
15. Was "User Agreement" read and signed? ☐ YES ☐ NO

SYSTEMS ACCESS INFORMATION (Check All applicable areas)

16. ☐ **SAAR: Network Access** (Check applicable box(es)) ☐ LAN ☐ EMAIL ☐ VPN/Dial-In

17. ☐ **UNIX**	USERID:	☐ Datastage:	Folder/Server:
	☐ Peacockd1 ☐ Greenjay ☐ KCAX09 ☐ Corncrake ☐ KCAX06 ☐ KCSU05 ☐ SULU		☐ Shell Login
18. ☐ **INFORMIX**	USERID:	Database:	Environment:
19. ☐ **DB-2**	USERID:	Database:	Environment:
20. ☐ **SYBASE**	USERID:	Database:	Environment:
21. ☐ **SQL**	USERID:	Database:	Server:
22. ☐ **Direct Connect**	☐ Transaction Group:		
23. ☐ READ ONLY	☐ WRITE ☐ INSERT ☐ UPDATE ☐ DELETE		
24. ☐ **CVS**	FULL PATH: *(i.e. /home/cvsroot/…)*		
25. ☐ **VSS**	Server:	Folder(s):	
26. ☐ **SCOP2 (FMS)**	NITC Mainframe ID:		
27. ☐ **SYSTEM36**	System Name:		
28. ☐ **NITC**	USERID:	☐ TSOA/B/C ☐ TSOK ☐ CORE	☐ **TRMS**
29. ☐ **GLS**	USERID:	Type:	
30. ☐ **ADPS**	USERID:	☐ Prod ☐ Dev COI:	Group(s):

31. ☐ **PFCS** ☐ View ☐ Modify ☐ Approve ☐ Superuser Approver:
Responsibility: ☐ GL ☐ BE ☐ Controller ☐ User ☐ Inquiry
Budget Levels: ☐ Budgetary Resources ☐ Application of Budgetary Resources ☐ Allot ☐ Allocate

FOR RD DATA WAREHOUSE PFCS CONTACT FSA SECURITY FOR INSTRUCTIONS

32. ☐ **NFC** USERID: POI Code(s): ORG: Agency: ☐FA or ☐CE
☐ Sensitive ☐ Non-sensitive ☐ Inquiry ☐ Update ☐ Entry ☐ Certify/Approve
☐ ABCO ☐ BLCO ☐ CADI ☐ CULPRIT ☐ DOTSE ☐ FEDSINQ ☐ FOCUS ☐ IRIS
☐ MASC ☐ PINQ ☐ PMSO ☐ PROP ☐ RETM ☐ RFQS ☐ RIFR ☐ SF279
☐ SPIN ☐ SPPS Web ☐ SPPS Mainframe ☐ TINQ ☐ TMGT ☐ TRAI ☐ UCFE
☐ **TRAVEL** OON: ORG: ☐ RELEASE AUTHORITY ☐ RELEASE VOUCHER
☐ **STARWEB** ☐ TIMEKEEPER/TRANSMIT ☐ ADMIN SPECIFY CONTACT POINT:
☐ **REPORTING CENTER** ☐ TUMS ☐ ADMIN ☐ LEAVE ERROR ☐ FINANCIAL ☐ EARN ☐ W-2
☐ PERSONNEL ☐ WORKFORCE ☐ DETAILS & SENSITIVE
☐ **FFIS:** ☐ **FDW:** ☐ Basic ☐ Payroll *IAS, HEAT, CPAIS, ACRWS, Complete AD-1143*

33. ☐ **EAS** E-Auth ID: OIP Code(s): Service Center:
Role(s):

FSA Security Officer Use Only		**FSA Security Officer Use Only**
34. ISSO Initials:	35. Supervisor Initials:	36. Security Tracking No.:

Example of FSA-13-A (Continued)

FSA-13A (09-17-07) Page 2 of 3

37. **CAIVRS**	☐ Admin	☐ Inquiry		
38. ☐ **HYPERION**	E-Auth ID:	NITC ID:	District:	St/CO Code:
	☐ Development	☐ Test	☐ Certification	☐ Production
Database:	Server:	Folder:	Group:	Role:
Reports:	☐ State only ☐ State and County ☐ DW1703CT(COE) ☐ County Office ☐ State/Vendor			
Print Name of Approving Official	Sign Approval of Business Application Sponsor		Date	

IDMS SYSTEMS- SELECT ONE FROM DATABASE, USER TYPE AND GROUP

39. DATABASE	SYSTEM
☐ MTPPRD	KCMO Production
☐ MTPAXT	KCMO Acceptance Testing
☐ Dictionary	MAXTEST
☐ Dictionary	MCDSACPT
☐ MTPTST	KCMO Test
☐ Dictionary	MTEST
☐ Dictionary	MCDSDEVL
☐ MTPDEV	MTEST
☐ MTPCD2	CD2 Production
☐ MTPGIM	GIMS Production
☐ MTPGAT	GIMS Acceptance Test
☐ MTPGDV	GIMS Test/Development
☐ MTPPCI	PCIMS Production
☐ PCIAXTST	Acceptance Testing
☐ PCIMSDEV	Development/Test
☐ PCIMSPT	Production Test
☐ PCIMSDT	Development Test
☐ PCITEST	PCIMS Test

40. USER TYPE

- ☐ Programmer
- ☐ Programmer Analyst
- ☐ Manager (Data base)
- ☐ Change Control (Migrations)
- ☐ IDD (Integrated Data Dictionary)
- ☐ DB Administrator
- ☐ DC Administrator
- ☐ Scheduler
- ☐ System Administrator
- ☐ OLP (Online Print Log)
- ☐ OPER
- ☐ OLQ (Online Query)
- ☐ DMLO (Data Manipulation Online)

41. GROUPS

- ☐ Centralized Disbursement System (CDS)
- ☐ CAS – Adjust Controls
- ☐ CAS – Inquiry
- ☐ CAS – Monitor Controls
- ☐ CASH – Inquiry
- ☐ CASH – Data entry
- ☐ CASH – Database Maintenance
- ☐ CCDB – Inquiry
- ☐ CCDB – Maintenance (Update)
- ☐ Financial Management System (FMS)
- ☐ GIMS – PRODUCTION
- ☐ PCIMS – BATCH PROCESSING
- ☐ PCIMS - MESSAGE UPDATE
- ☐ **APLUS** – Basic (BAS)
- ☐ Create/Modify Agreements (232)
- ☐ Delete Agreements (227)
- ☐ Bank Reference File (247)
- ☐ Budget (231)
- ☐ Create/Modify Collections (238)
- ☐ Commodity Reference File (243)
- ☐ Commodity Supplier Ref. File (242)
- ☐ Country/Country Name Ref. File (246)
- ☐ Create/Modify Disbursements (237)
- ☐ Create/Modify Letter of Commitment (235)
- ☐ Delete Letter of Commitment (236)
- ☐ Month end Processing (240)
- ☐ Create/Modify PA/SALES (233)
- ☐ Delete PA/SALES (228)
- ☐ Port Reference File (244)
- ☐ Create/Modify Rescheduling (239)
- ☐ System Parameters Reference File-ASCS (248)
- ☐ System Parameters Reference File- FAS (241)
- ☐ Create/Modify Vessel Approvals (234)
- ☐ Delete Vessel Approvals (229)
- ☐ Vessel Supplier Reference File (245)
- ☐ Remove Funds (249)
- ☐ Change Request (250)

42. AS/400	☐ User	☐ Master	☐ Communications	☐ Other:

43. Other:

44. Justification:

45A. Print Supervisor Name	45B. Phone No. *(Include Area Code):*
45C. Supervisor Signature	45D. Date *(MM-DD-YYYY):*

FSA SECURITY OFFICE USE ONLY

46A. ISSO/SLR Signature	46B. Date *(MM-DD-YYYY)*	47. Security Staff Tracking No.

Example of FSA-13-A (Continued)

FSA-13-A (09-17-07) Page 3 of 3

ITEM NO	COMPLETION INSTRUCTIONS	
	ITEMS 1-15 ARE REQUIRED FOR ALL REQUEST TYPES	
1	Request Date	Enter the date you submit the request for the FSA Security Office
2	Request Type	Check the box which is applicable to the type of request
3	Last Name	Enter last name
4	Full Legal Name	Enter full legal name
5	Full Organizational Acronym	Provide your full organizational acronym, for example DAM/ITSD/OTC
6	Room/Cube No.	Provide your Room or Cube number if applicable
7	Phone No.	Provide your Phone number including Area Code
8	Fax No.	Provide your Fax number including Area Code
9	Email Address	Provide your Email Address
10	Request Effective Date	Enter the Effective Date, or Start Date
11	Employee Type	Identify your appropriate employee type
12	Temporary Access	Check 'YES' if Temporary Access request. If yes, enter Termination Date for Access
13	Background Investigation	Check 'YES' or 'NO', if a "Background Investigation" was performed, (or in process)
14	Security Awareness	Check 'YES' or 'NO', if "Security Awareness Training" was completed
15	User Agreement	Check 'YES' or 'NO', if "User Agreement" was read and signed
	SYSTEM ACCESS INFORMATION	
16	SAAR	Select appropriate action for LAN, EMAIL, or VPN/Dial-In
17	UNIX	Enter user ID, Select Server; enter Folder if Datastage is needed
18	INFORMIX	Enter user ID, Database name, Environment (i.e. Production, Acceptance Test, Development)
19	DB-2	Enter user ID, Database name, Environment (i.e. Production, Acceptance Test, Development)
20	SYBASE	Enter user ID, Database name, Environment (i.e. Production, Acceptance Test, Development)
21	SQL	Enter user ID, Database name, Server name
22	Direct Connect	Select if needed for DB2, enter Transaction Group
23	Access Level	Select level of access for UNIX, DB2, SQL
24	CVS	Enter FULL path of CVS database
25	VSS	Visual Source Safe, enter Server name and Folder names
26	SCOP2 (FMS)	Enter NITC mainframe user id
27	SYSTEM36	Enter system name needed
28	NITC	Enter user ID, select TSO level, CORE (list regions in "OTHER"), TRMS if needed
29	GLS	Enter NITC user ID, Type (i.e. District, EFT…)
30	ADPS	Enter user ID, Select Production or Development
31	PFCS	Select Level, enter your Approver. Responsibility, choose GL and/or BE and Type. Select range of Budget Levels
32	NFC	Enter user ID, POI and ORG code(s), Agency. Select all applicable sub-systems
33	EAS	Enter e-Auth user ID, OIP code(s), Role names
34	ISSO Initials	FOR FSA Security Office USE ONLY
35	Supervisor Initials	**REQUIRED**, supervisor must initial they have reviewed Page 1
36	Security Tracking No.	FOR FSA Security Office USE ONLY
37	CAIVRS	
38	HYPERION	Enter e-Auth user ID, NITC user id, District, St/Co Code, Environment, Database, Server, Group, and Role. Select required reports. **MUST** submit to Datamart Owner for Approval Prior to submitting to FSA Security.
	IDMS SYSTEMS	
39-41	IDMS Systems	Select at least 1 Database, Applicable User type(s) and ALL Applicable Group(s)
42	AS/400	Select User, Master, Communications or Other. If other, specify.
43	Other	Write in other access for above access, or if not specified above
44	Justification	Business justification for access
45A	Print Supervisor Name	Legibly print supervisor name
45B	Phone No.	Supervisor phone number
45C	Supervisor Signature	Signature of supervisor (Branch Chief or above)
45D	Date	Date signed by supervisor
46A	ISSO/SLR Signature	FOR FSA Security Office USE ONLY
46B	Date	FOR FSA Security Office USE ONLY
47	Security Staff Tracking No.	FOR FSA Security Office USE ONLY

WHERE TO SUBMIT SECURITY ACCESS REQUEST FORM, FSA-13A
FSA Information Security Office
Phone: 816-926-6537
FAX: 816-627-0687 or 816-926-6090
email: security@kcc.usda.gov

FSA-13-A Instructions

The following provides instructions for completing FSA-13-A.

Completing FSA-13-A **Notes:** Items 1-15, 35, and 45 A-D must **always** be completed. Items 16, 27-30, 32, 33, 38, 39, and 42 will be completed depending on what access an employee needs.	
IF access is needed for...	**THEN complete the following...**

Automated Data Processing System (ADPS)
 	
Note: IT will contact County Office to assist County Master Security Officer in setting up user ID and password.
	• item 30:
	
	  • CHECK "**ADPS**"
	  • for USERID:, enter NITC user ID, if available
	
	• item 43, list the Counties for which access is needed.

AS/400	item 42, check the following items that apply: • "**User**" • "**Master**".
Credit Alert Interactive Voice Response System (CAIVRS)	item 37, CHECK "**Inquiry**".
Conservation-CRP DCP Farm Records ManagementS (FRMS) Land Value Survey (LVS) National Payment System (NPS) SCIMS Subsidiary	item 33: • CHECK "**EAS**" • for E-Auth ID:, enter eAuthentication ID • for Service Center:, enter name of counties for which access is needed; if more space is needed use item 43 • for Role(s):, enter roles from item 33 or leave blank if role needed is Farm Records Management, DCP, or Subsidiary.

e-mail, local area network (LAN), or virtual private network (VPN)	item 16:
	
	• CHECK "**SAAR**"
	• check any of the following:
	
	  • "**LAN**"
	  • "**EMAIL**"
	  • "**VPN/Dial-In**".

Guaranteed Loan System (GLS)	item 29: • CHECK "**GLS**" • for USERID:, enter NITC user ID, if available • for Type:, ENTER "**County**".

FSA-13-A Instructions (Continued)

IF access is needed for...	THEN complete the following...

HYPERION	item 38:
	
	• CHECK "**HYPERION**"
	• for E-Auth ID:, enter eAuthentication ID
	• for NITC ID:, enter CA ID
	• for District:, enter District Number
	• for St/CO Code:, enter State and county code
	• for Folder:, enter "**Office Data Mart**".
	• for Group:, enter "**County**"
	• for Reports, check the following:
	
	  • "**DW1703CT(COE)**"
	  • "**County Office**".

NFC **Note:** If NFC is needed, and it is the first time the request is made, NITC must also be chosen.	item 32: • CHECK "**NFC**" • for USERID:, enter NITC user ID, if available.
NITC **Note:** NITC must be checked if requesting NFC for the first time.	item 28: • CHECK "**NITC**" • for USERID:, enter NITC user ID, if available.
PINQ	item 32, check the following: • "**Non-Sensitive**" or "**Sensitive**" • "**PINQ**".

System for Time and Attendance Reporting (STAR) WEB	item 32
	
	• check the following:
	
	  • "**STARWEB**"
	  • "**TIMEKEEPER/TRANSMIT**"
	
	• for **SPECIFY CONTACT POINT:**, enter users City/Town code.

System 36	item 27, CHECK "**SYSTEM36**" **Note:** IT will contact County Office to assist County Master Security Officer in setting up user ID and password.

FSA-13-A Instructions (Continued)

IF access is needed for...	THEN complete the following...

TRAVEL	• item 32:
	  • for Agency, check either of the following:
	  • "**FA**"
	  • "**CE**"
	  Note: FA is Federal and CE is County.
	  • check the following items that apply:
	  • "**Inquiry**"
	  • "**Entry**"
	  • "**RELEASE AUTHORITY**"
	  • "**RELEASE VOUCHER**".
	• item 43, enter counties for which access is needed.

Telecommunications Resource Management System (TRMS)	• item 28:
	  • check the following:
	  • "**NITC**"
	  • "**TRMS**"
	  • for USERID:, enter NITC user, if available
	• item 43, enter the counties for which access is needed.

General notes and information:

- CAIVRS passwords are good for 21 calendar days, to continue using the password, it must be reset before it expires.
- Electronic Repository System Request (ERSR) access requests for NFC take 1 ½ to 3 weeks. Password resets take less than 24 hours.
- GLS and NITC use the same password. When user changes 1 password, the system changes the other password.
- Login ID not completed; if user receives the error message, "Login ID xxxxx login not completed", the system is busy, try again later.
- NFC and STAR WEB use the same ID and password. When user changes 1 password, the system changes the other password.
- NFC's password cycle is 90 calendar days. If an ID is inactive for 60 calendar days it is suspended, if it is inactive for 90 calendar days it is deleted.
- NITC's password cycle is 35 calendar days. If an ID is inactive for 120 calendar days it is suspended, if it is inactive for 180 calendar days it is deleted.

FSA-13-A shall be submitted to SLR for additions, changes, or deletions.

FSA Systems, System Access Requirements, and Contacts for Access Issues

The following provides FSA systems, system access requirements, and contacts for access issues.

Passwords are required for the following.	FSA-13-A Required	Who/What Establishes Access	Problem	Contacts
ADPS	√	SLR through ERSR.	If access is needed for additional counties.	Submit FSA-13-A.
			Password Reset	ISOS 800-255-2434, option 2 or SLR.
AgLearn		Any employee with eAuthentication login.	Login or password.	**eAuthenticationhelpdesk @ ftc.usda.gov** or ISOS 800-255-2434, option 3.
AS/400	√	SLR to ITS to County Office - Administrator/ Master Security Officer.	Master password reset.	SLR must call ISOS.
CAIVRS	√	SLR through ERSR.		
CLU, Geo Data, shared drives.		SLR to SAAR Magic Ticket to ITS.		
eAuthentication		Employee, go to **http://intra4.fsa.usda.gov/KY/KYi/Kentucky/eGov.htm**.	Login or password, account usage, and account maintenance.	Self Help through **eAuthenticationhelpdesk @ ftc.usda.gov**
E-mail	√	SLR to SAAR Magic Ticket to ITS.	If problems after initial setup.	ITS Service Center
EmpowHR		ADM/HR.	Password Reset.	SLR
Farm Business Plan		eAuthentication.	Obtaining access.	SLR grants access once they receive the following information: • employee e-mail address • name • location • eAuthentication ID.
FedTraveler		eAuthentication.		**eAuthenticationhelpdesk @ ftc.usda.gov** or Travel coordinator.
FSA Intranet - LAN initial setup	√	SLR to SAAR Magic Ticket to ITS.	If problems after initial setup.	ITS Service Center.

FSA Systems, System Access Requirements, and Contacts for Access Issues (Continued)

Passwords are required for the following.	FSA-13-A Required	Who/What Establishes Access	Problem	Contacts
HYPERION	√	eAuthentication and FSA-13-A sent to SLR to Datamart Contact to Security Office.	Password reset eAuthentication.	Go to **eAuthenticationhelpdesk @ftc.usda.gov**. Requires name, daytime phone number, and brief description of problem.
			If prompts for 2nd password.	ISOS 800-255-2434, option 2.
NFC Personal Page		Employee.		**www.nfc.usda.gov**
NFC: TRAVEL	√	SLR through ERSR.	NFC password reset.	ISOS 800-255-2434, option 2 or SLR. If deleted requires FSA-13-A.
NITC: GLS, TRMS	√	SLR through ERSR.	NITC password reset.	ISOS 800-255-2434, option 2 or SLR. If deleted requires FSA-13-A.
NPS	√	FSA-13-A to SLR to ISOS.	Login or password is eAuthentication.	Self-help through **http://intra4.fsa.usda.gov/ KY/KYi/Kentucky/eGov.htm**.
PCMS		Administrative Division.	PCMS password reset.	SLR.
Personal PC Workstation	√	SLR to SAAR Magic Ticket to ITS.	If problems after initial setup.	ITS Service Center.
SCIMS	√	FSA-13-A, 1-CM, AD-2017, to SLR through the SCIMS Officer to Security Office.	Login or password is eAuthentication.	State SCIMS Security Officer.
STARWEB	√	SLR through ERSR.	STAR WEB password reset.	ISOS 800-255-2434, option 2. If deleted, requires FSA-13-A.
System 36	√	SLR to IT to County Office-Administrator/ Master Security Officer.		ITS Service Center.
Thrift		Employee.		**www.tsp.gov**.

FSA Roles for Completing FSA-13-A, Item 38

The following provides data to complete FSA-13-A, item 38.

System Name	System Abbreviation	Role	Approver	Assign	Additional Info
Conservation - CRP	COTS/COLS	app.fsa.gsop.signupadmin	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and Office Information Profile (OIP)	
Direct and Counter-Cyclical Payment Program	DCP		eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	OIP	
Electronic Funds Control	EFUNDS		Must have approval from designated large office staff.	Role and OIP	FMD, Payment Management Office (PMO); FMD, Project Management Center (PMC); or Accounting Policy and Standards Office (APSO) must approve this access.
		app.fsa.efc.grp.ALL	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.grp.ALL.READONLY	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.grp.CONSERVATION	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.grp.CONSERVATION.READONLY	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.grp.FMD	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.grp.FMD.READONLY	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.grp.PECD.DISASTER	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, APSO, or PECD must approve this access.
		app.fsa.efc.grp.PECD.READONLY	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, APSO, or PECD must approve this access.
		app.fsa.efc.grp.PECD.REGULAR	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, APSO, or PECD must approve this access.
		app.fsa.efc.grp.PEDC.Section32	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, APSO, or PECD must approve this access.
		app.fsa.efc.grp.PRICE.SUPPORT	Must have approval from designated large office staff.	Role and OIP	
		app.fsa.efc.grp.PRICE.SUPPORT.READONLY	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.

FSA Roles for Completing FSA-13-A, Item 38 (Continued)

System Name	System Abbreviation	Role	Approver	Assign	Additional Info
Electronic Funds Control (Cntd)	EFUNDS (Cntd)	app.fsa.efc.grp.TOBACCO	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.grp.TOBACCO.READONLY	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.rol.CSCR	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.rol.FM	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.rol.NPM	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.rol.NSCR	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.rol.SPM	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
		app.fsa.efc.rol.SSCR	Must have approval from designated large office staff.	Role and OIP	PMO, PMC, or APSO must approve this access.
	PRICE SUPPORT	app.fsa.PriceSupport	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
Electronic Loan Deficiency Payment Service	ELDP	app.fsa.eLDP.Inquiry	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.fsa.eLDP.RateAdmin	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.fsa.eLDP.Superuser	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
Farm Loan and Direct Loan System	FLP and DLS	app.fsa.flp.dls.sc	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.so	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.do	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.no	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.fo	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.hd	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.it	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	

FSA Roles for Completing FSA-13-A, Item 38 (Continued)

System Name	System Abbreviation	Role	Approver	Assign	Additional Info
Farm Loan and Direct Loan System (Cntd)	FLP and DLS (Cntd)	app.fsa.flp.dls.nf	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.view	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.report	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.lm	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.ls	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.lm.cm	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.1a.manuscript	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.1a.submit	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.1c	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.1d	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.1f	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.1m	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.4a	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.4d	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.5f	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.8r	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.dls.plas.9g	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.sala.analyst	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.sala.expert	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		EAS Attribute Assignments			
		app.fsa.flp.office	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
		app.fsa.flp.1a.office	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP and Attribute	
Farm Loan Program	FLPRA	app.fsa.flp.flpra.admin	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
Farm Records Manageme nt System	FRMS			OIP	County Office (Service Center) User
		app.fsa.frs.ac	Must be approval and submitted by Sandy Bryant	Role and OIP	State Office User
		app.fsa.frs.national	Must be approval and submitted by Sandy Bryant	Role and OIP	National Office User
Food and Agricultura l Import Regulations and Standards	FAIRS	app.fsa.fairs.Certify	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.fsa.fairs.Lookup	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.fsa.fairs.superuser	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.fsa.fairs.Update	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	

FSA Roles for Completing FSA-13-A, Item 38 (Continued)

System Name	System Abbreviation	Role	Approver	Assign	Additional Info
Land Value Survey	LVS	app.fsa.lvs.readonly	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.lvs.national.inquiry	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.lvs.national.restricted	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.lvs.national.update	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.lvs.state	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
LRA - EAUTH	LRA	OCIO_LRATraining_FSA_Employee	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	eAuthentication Role	
Milk Income Loss Contract	MILCX	app.fsa.PriceSupport	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
National Crop Table	NCT	app.fsa.nct.cty	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.fsa.nct.state	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		app.fsa.nct.reset	Must have approval from designated large office staff.	Role and OIP	
National Payment Services	NPS	FS.P.AFAO.ROLE.CtyCertOff	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	Will not work if they have a State OIP
		FS.P.AFAO.ROLE.CtySignOff	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	Will not work if they have a State OIP
		FS.P.AFAO.ROLE.NatSampCoord	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		FS.P.AFAO.ROLE.NatSignOff	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	
		FS.P.AFAO.ROLE.StCertOff	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	Will not work if they have a County OIP.
		FS.P.AFAO.ROLE.StRep	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	Will not work if they have a County OIP.
		FS.P.AFAO.ROLE.StSignOff	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	Will not work if they have a County OIP.
		FS.P.AFAO.ROLE.SvcCtrRep	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	Will not work if they have a State OIP
	SOILS	app.fsa.sdms.update	eAuthentication coordinator, SCIMS coordinator, or SLR must approve.	Role and OIP	

FSA Roles for Completing FSA-13-A, Item 38 (Continued)

System Name	System Abbreviation	Role	Approver	Assign	Additional Info
Service Center Information Management System	SCIMS	SCIMS.PARMO.rol.PYBC	SCIMS Coordinator and SLR must have National Office approval.	Role and OIP	Must have AD-2017 with the approved SCIMS spreadsheet per Notice CM-560 for submitting to FSA Security.
		SCIMS.PARMO.rol.readonly	SCIMS Coordinator and SLR must have National Office approval.	Role and OIP	Must have AD-2017 with the approved SCIMS spreadsheet per Notice CM-560 for submitting to FSA Security.
		SCIMS.PARMO.rol.update	SCIMS Coordinator and SLR must have National Office approval.	Role and OIP	Must have AD-2017 with the approved SCIMS spreadsheet per Notice CM-560 for submitting to FSA Security.
		app.fsa.scims.activedate	SCIMS Coordinator and SLR must have National Office approval.	Role and OIP	Must have AD-2017 with the approved SCIMS spreadsheet per Notice CM-560 for submitting to FSA Security.
		app.fsa.scims.federalids	SCIMS Coordinator and SLR must have National Office approval.	Role and OIP	Must have AD-2017 with the approved SCIMS spreadsheet per Notice CM-560 for submitting to FSA Security.
Subsidiary	WEB ELIGIBILITY		SCIMS Coordinator and SLR must have National Office approval.	OIP	Must have AD-2017 with the approved SCIMS spreadsheet per Notice CM-560 for submitting to FSA Security.