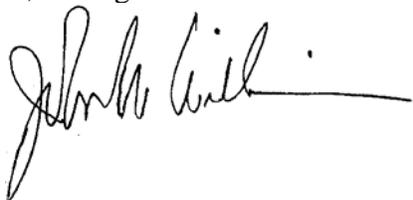


For: FSA Employees and Contract Employees

FSA Computer Security Procedures

Approved by: Deputy Administrator, Management



1 Overview

A Background

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

In FY 2006, FSA had an independent audit review by PricewaterhouseCoopers (PwC) that determined that improvements could be made in security access request processes and training. FSA is required to address the issues raised by PwC about security access request procedures and forms. FSA management and the Information Security Office (ISO) determined that ISO would:

- review current procedures and forms used in FSA’s processes for collecting, processing, and controlling information security access requests
- improve security access requests procedures.

This notice will affect all information security access requests for all FSA employees and contractors.

All managers (supervisors and Contracting Officer’s Technical Representatives (COTR’s)) have a significant responsibility to ensure that:

- procedures are followed
- forms are filled out completely and returned to the correct offices.

<p>Disposal Date</p> <p>October 1, 2007</p>	<p>Distribution</p> <p>All FSA employees and contractors; State Offices relay to County Offices</p>
--	--

Notice IRM-382

1 Overview (Continued)

B Purpose

This notice provides procedures and forms for requesting computer security access privileges, granted by or through ISO (who oversees Information Security Operation Support (ISOS)), to all systems that all FSA employees, contract employees, and partners (collectively referred to as “user”, “requester”, and “individual”) may need in the performance of their duties. Users **must** comply with these procedures in addition to all other applicable Federal, USDA, FSA, and OCIO ITS requirements.

C Sources of Authority

The sources of authority are:

- 6-IRM
- Notice IRM-367
- Notice IRM-370
- USDA Cyber Security Manual Series 3500 and associated Cyber Security guidance
- USDA Administrative Bulletin Departmental Regulation (DR) 3602-001, OCIO-ITS Security Policy Manual
- 2-PM
- 27-PM.

2 Responsibilities

A Supervisor/COTR Responsibilities

It is the responsibility of each supervisor/COTR, who is signing FSA-13-A (Exhibit 1), to determine who should be granted access **privileges** to electronic record systems, and to:

- confirm that the individual has signed FSA-13
- complete and submit FSA-13-A to the Security Liaison Representative (SLR)/FSA ISOS
- confirm that 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 the Initial Security Awareness Training to the SLR/ISOS

2 Responsibilities (Continued)

A Supervisor/COTR Responsibilities (Continued)

- **submit FSA-13-A beforehand, 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.**

Note: If FSA-13-A is **not** submitted to SLR/ISOS, a user's personal 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.

Individuals will be provided with initial 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 Notices IRM-367 and IRM-370.

The "Security Expectations and Rules of Behavior" flyer is available at either of the following:

- **ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures/SecurityExpectationsFlyer_Final.pdf**
- **ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures/SecurityExpectationsFlyer_VisuallyImpairedVersion_Final.doc**

The "Security Incident Response Guide for Users" is available at either of the following:

- **<ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures/SecurityIncidentResponseGuide.pdf>**
- **ftp://ftp-fc.sc.egov.usda.gov/ITC/SecurityBrochures/SecurityIncidentResponseGuide_508.doc**

Notes: FSA-13-A's are:

- required for access requests for 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
- requested through ISOS.

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

2 Responsibilities (Continued)

B SLR Responsibilities

SLR's are responsible for:

- 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:

- 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.

D Individual Granted Access to Secure Systems Responsibilities

It is the responsibility of each individual, in which management grants the privilege to access an electronic data system, who is requesting access to FSA systems and data to:

- read and sign FSA-13 and submit to the user's manager
- complete and submit FSA-13-A to their manager
- confirm that a background check has been requested from HRD or their Administrative Officer
- confirm to supervisor/COTR that the individual has completed the Initial Security Awareness Training according to subparagraph A.

Notice IRM-382

3 Procedures

A Large Offices Procedures

Large offices include the National Office; Kansas City, Missouri; St. Louis, Missouri; and the Aerial Photography Field Office.

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 the FSA 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 (10-25-06)

FSA-13-A:

- is the **only** acceptable system access request format for privileges
- will replace FSA-13B's, FSA-13C's, KC-328's, and KC-330's. SLR's and ISOS will no longer accept FSA-13B's, FSA-13C's, KC-328, or KC-330's. Completed FSA-13-A's should be submitted by FAX to 816-926-6090.

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

- e-mail to security@kcc.usda.gov
- telephone at 816-926-6537.

FSA-13-A (10-25-06)

This is an example of FSA-13-A.

<p>This form is available electronically.</p>		<p>See Page 3 for Completion Instructions.</p>	
<p>FSA-13-A (10-25-06)</p>		<p>U.S. DEPARTMENT OF AGRICULTURE Farm Service Agency</p>	
<p>DATA SECURITY ACCESS AUTHORIZATION FORM</p>		<p>INSTRUCTIONS: Please complete a separate form for each employee. Items 1 through 20 MUST be completed.</p>	
<p>1. Request Date:</p>		<p>2. Request Type: <input type="checkbox"/> ADD <input type="checkbox"/> MODIFY <input type="checkbox"/> DELETE</p>	
<p>3. Last Name</p>		<p>4. Full Legal Name (Including middle and suffix)</p>	
<p>5. Social Security Number</p>		<p>6. Office</p>	
<p>7. Division</p>		<p>8. Branch/Section</p>	
<p>9. Room No.</p>		<p>10. Phone No. (Include Area Code)</p>	
<p>11. Fax No. (Include Area Code)</p>		<p>12. Email Address</p>	
<p>13. Effective Date:</p>		<p>14. Separation Date:</p>	
<p>15. Employee Type (Check applicable box): <input type="checkbox"/> KC <input type="checkbox"/> STL <input type="checkbox"/> WDC <input type="checkbox"/> ST/CO <input type="checkbox"/> CONTRACTOR <input type="checkbox"/> OTHER (Specify):</p>			
<p>16. Temporary Access <input type="checkbox"/> YES <input type="checkbox"/> NO</p>			
<p>17. Termination Date of Temporary Access</p>			
<p>18. Background Investigation <input type="checkbox"/> YES <input type="checkbox"/> NO</p>			
<p>19. Security Awareness <input type="checkbox"/> YES <input type="checkbox"/> NO</p>			
<p>20. User Agreement <input type="checkbox"/> YES <input type="checkbox"/> NO</p>			
<p>SYSTEMS ACCESS INFORMATION (Check All applicable areas)</p>			
<p>21. <input type="checkbox"/> SAAR: Network Access (Check applicable box(es)) <input type="checkbox"/> LAN <input type="checkbox"/> EMAIL <input type="checkbox"/> VPN/Dial-In</p>			
<p>22. <input type="checkbox"/> UNIX</p>		<p>USERID: <input type="checkbox"/> SCITDW01 <input type="checkbox"/> Greenjay <input type="checkbox"/> KCAX09 <input type="checkbox"/> Corncrake <input type="checkbox"/> Shell Login <input type="checkbox"/> KCAX06 <input type="checkbox"/> KCSU05 <input type="checkbox"/> SULU</p>	
<p>23. <input type="checkbox"/> INFORMIX</p>		<p>USERID: Database: Environment:</p>	
<p>24. <input type="checkbox"/> DB-2</p>		<p>USERID: Database: Environment:</p>	
<p>25. <input type="checkbox"/> SYBASE</p>		<p>USERID: Database: Environment:</p>	
<p>26. <input type="checkbox"/> SQL</p>		<p>USERID: Database: Server:</p>	
<p>27. <input type="checkbox"/> Direct Connect <input type="checkbox"/> Transaction Group:</p>			
<p>28. <input type="checkbox"/> READ ONLY <input type="checkbox"/> WRITE <input type="checkbox"/> INSERT <input type="checkbox"/> UPDATE <input type="checkbox"/> DELETE</p>			
<p>29. <input type="checkbox"/> CVS PATH: (i.e. /home/cvsroot/...)</p>			
<p>30. <input type="checkbox"/> VSS Server: Folder(s):</p>			
<p>31. <input type="checkbox"/> SCOP2 (FMS) Mainframe ID:</p>			
<p>32. <input type="checkbox"/> SYSTEM36 System:</p>			
<p>33. <input type="checkbox"/> NITC USERID: <input type="checkbox"/> TSOA/B/C <input type="checkbox"/> TSOK <input type="checkbox"/> CORE <input type="checkbox"/> TRMS</p>			
<p>34. <input type="checkbox"/> GLS USERID: Type:</p>			
<p>35. <input type="checkbox"/> ADPS USERID: <input type="checkbox"/> Prod <input type="checkbox"/> Dev COI: Group(s):</p>			
<p>36. <input type="checkbox"/> PFCS <input type="checkbox"/> View <input type="checkbox"/> Modify <input type="checkbox"/> Approve <input type="checkbox"/> Superuser Approver: Responsibility: <input type="checkbox"/> GL <input type="checkbox"/> BE <input type="checkbox"/> Controller <input type="checkbox"/> User <input type="checkbox"/> Inquiry Budget Levels: <input type="checkbox"/> Budgetary Resources <input type="checkbox"/> Application of Budgetary Resources <input type="checkbox"/> Allot <input type="checkbox"/> Allocate</p>			
<p>FOR RD DATA WAREHOUSE PFCS CONTACT FSA SECURITY FOR INSTRUCTIONS</p>			
<p>37. <input type="checkbox"/> NFC USERID: POI Code(s): ORG: Agency: <input type="checkbox"/> FA or <input type="checkbox"/> CE <input type="checkbox"/> Sensitive <input type="checkbox"/> Non-sensitive <input type="checkbox"/> Inquiry <input type="checkbox"/> Update <input type="checkbox"/> Entry <input type="checkbox"/> Certify/Approve <input type="checkbox"/> ABCO <input type="checkbox"/> BLCO <input type="checkbox"/> CADI <input type="checkbox"/> CULPRIT <input type="checkbox"/> DOTSE <input type="checkbox"/> FEDSINQ <input type="checkbox"/> FOCUS <input type="checkbox"/> IRIS <input type="checkbox"/> MASC <input type="checkbox"/> PINQ <input type="checkbox"/> PMSO <input type="checkbox"/> PROP <input type="checkbox"/> RETM <input type="checkbox"/> RFQS <input type="checkbox"/> RIFR <input type="checkbox"/> SF279 <input type="checkbox"/> SPIN <input type="checkbox"/> SPPS Web <input type="checkbox"/> SPPS Mainframe <input type="checkbox"/> TINQ <input type="checkbox"/> TMGT <input type="checkbox"/> TRAI <input type="checkbox"/> UCFE <input type="checkbox"/> TRAVEL OON: ORG: <input type="checkbox"/> RELEASE AUTHORITY <input type="checkbox"/> RELEASE VOUCHER <input type="checkbox"/> STARWEB <input type="checkbox"/> TIMEKEEPER/TRANSMIT <input type="checkbox"/> ADMIN SPECIFY CONTACT POINT: <input type="checkbox"/> REPORTING CENTER <input type="checkbox"/> TUMS <input type="checkbox"/> ADMIN <input type="checkbox"/> LEAVE ERROR <input type="checkbox"/> FINANCIAL <input type="checkbox"/> EARN <input type="checkbox"/> W-2 <input type="checkbox"/> PERSONNEL <input type="checkbox"/> WORKFORCE <input type="checkbox"/> DETAILS & SENSITIVE <input type="checkbox"/> FFIS: <input type="checkbox"/> FDW: <input type="checkbox"/> Basic <input type="checkbox"/> Payroll IAS, HEAT, CPAIS, ACRWS, Complete AD-1143</p>			
<p>38. <input type="checkbox"/> EAS E-Auth ID: OIP Code(s): Service Center: Role(s):</p>			
<p>39. ISSO Initials:</p>		<p>40. Supervisor Initials:</p>	
<p>41. Security Tracking No.:</p>			

FSA-13-A (10-25-06) (Continued)

FSA-13A (10-25-06)		Page 2 of 3	
42. CAIVRS	<input type="checkbox"/> Admin	<input type="checkbox"/> Inquiry	
43. <input type="checkbox"/> HYPERION	E-Auth ID:	NITC ID:	District:
	<input type="checkbox"/> Development	<input type="checkbox"/> Test	<input type="checkbox"/> Certification
Database:	Server:	Folder:	Group:
Reports:	<input type="checkbox"/> State only	<input type="checkbox"/> State and County	<input type="checkbox"/> DW1703CT(COE)
		<input type="checkbox"/> County Office	<input type="checkbox"/> State/Vendor
Print Name of Approving Official		Sign Approval of Business Application Sponsor	
		Date	
IDMS SYSTEMS- SELECT ONE FROM DATABASE, USER TYPE AND GROUP			
44. DATABASE <input type="checkbox"/> MTPPRD <input type="checkbox"/> MTPAXT <input type="checkbox"/> Dictionary <input type="checkbox"/> Dictionary <input type="checkbox"/> MTPST <input type="checkbox"/> Dictionary <input type="checkbox"/> Dictionary <input type="checkbox"/> MTPDEV <input type="checkbox"/> MTPCD2 <input type="checkbox"/> MTPGIM <input type="checkbox"/> MTPGAT <input type="checkbox"/> MTPGDV <input type="checkbox"/> MTPPCI <input type="checkbox"/> PCIAXTST <input type="checkbox"/> PCIMSDEV <input type="checkbox"/> PCIMSPT <input type="checkbox"/> PCIMSDT <input type="checkbox"/> PCITEST	SYSTEM KCMO Production KCMO Acceptance Testing MAXTEST MCDSACPT KCMO Test MTEST MCDSDEVL MTEST CD2 Production GIMS Production GIMS Acceptance Test GIMS Test/Development PCIMS Production Acceptance Testing Development/Test Production Test Development Test PCIMS Test	46. GROUPS <input type="checkbox"/> Centralized Disbursement System (CDS) <input type="checkbox"/> CAS – Adjust Controls <input type="checkbox"/> CAS – Inquiry <input type="checkbox"/> CAS – Monitor Controls <input type="checkbox"/> CASH – Inquiry <input type="checkbox"/> CASH – Data entry <input type="checkbox"/> CASH – Database Maintenance <input type="checkbox"/> CCDB – Inquiry <input type="checkbox"/> CCDB – Maintenance (Update) <input type="checkbox"/> Financial Management System (FMS) <input type="checkbox"/> GIMS - PRODUCTION <input type="checkbox"/> PCIMS – BATCH PROCESSING <input type="checkbox"/> PCIMS - MESSAGE UPDATE <input type="checkbox"/> APLUS – Basic (BAS) <input type="checkbox"/> Create/Modify Agreements (232) <input type="checkbox"/> Delete Agreements (227) <input type="checkbox"/> Bank Reference File (247) <input type="checkbox"/> Budget (231) <input type="checkbox"/> Create/Modify Collections (238) <input type="checkbox"/> Commodity Reference File (243) <input type="checkbox"/> Commodity Supplier Ref. File (242) <input type="checkbox"/> Country/Country Name Ref. File (246) <input type="checkbox"/> Create/Modify Disbursements (237) <input type="checkbox"/> Create/Modify Letter of Commitment (235) <input type="checkbox"/> Delete Letter of Commitment (236) <input type="checkbox"/> Month end Processing (240) <input type="checkbox"/> Create/Modify PA/SALES (233) <input type="checkbox"/> Delete PA/SALES (228) <input type="checkbox"/> Port Reference File (244) <input type="checkbox"/> Create/Modify Rescheduling (239) <input type="checkbox"/> System Parameters Reference File-ASCS (248) <input type="checkbox"/> System Parameters Reference File- FAS (241) <input type="checkbox"/> Create/Modify Vessel Approvals (234) <input type="checkbox"/> Delete Vessel Approvals (229) <input type="checkbox"/> Vessel Supplier Reference File (245) <input type="checkbox"/> Remove Funds (249) <input type="checkbox"/> Change Request (250)	
45. USER TYPE <input type="checkbox"/> Programmer <input type="checkbox"/> Programmer Analyst <input type="checkbox"/> Manager (Data base) <input type="checkbox"/> Change Control (Migrations) <input type="checkbox"/> IDD (Integrated Data Dictionary) <input type="checkbox"/> DB Administrator <input type="checkbox"/> DC Administrator <input type="checkbox"/> Scheduler <input type="checkbox"/> System Administrator <input type="checkbox"/> OLP (Online Print Log) <input type="checkbox"/> OPER <input type="checkbox"/> OLQ (Online Query) <input type="checkbox"/> DMLO (Data Manipulation Online)			
47. AS/400	<input type="checkbox"/> User	<input type="checkbox"/> Master	<input type="checkbox"/> Communications
<input type="checkbox"/> Other:			
48. Other:			
49. Justification:			
50A. Print Supervisor Name		50B. Phone No. (Include Area Code):	
50C. Supervisor Signature		50D. Date (MM-DD-YYYY):	
51A. ISSO/SLR Signature	51B. Date (MM-DD-YYYY)	52. Security Staff Tracking No.	

FSA-13-A (10-25-06) (Continued)

FSA-13-A (10-25-06)		Page 3 of 3
ITEM NO	COMPLETION INSTRUCTIONS	
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	Social Security No.	Provide your Social Security Number
6	Office	Provide your Office acronym
7	Division	Provide your Division acronym
8	Branch/Section	Provide your Branch/Section acronym
9	Room No.	Provide your Room number
10	Phone No.	Provide your Phone number including Area Code
11	Fax No.	Provide your Fax number including Area Code
12	Email Address	Provide your Email Address
13	Effective Date	Enter the Effective Date, or Start Date
14	Separation Date	Enter the Separation Date, if separating from the Agency
15	Employee Type	Identify your appropriate employee type
16	Temporary Access	Check 'YES' or 'NO', if "Temporary Access"
17	Termination Date of Temporary Access	Enter the Termination Date of Temporary Access
18	Background Investigation	Check 'YES' or 'NO', if a "Background Investigation" was performed, (or in process)
19	Security Awareness	Check 'YES' or 'NO', if "Security Awareness Training" was completed
20	User Agreement	Check 'YES' or 'NO', if "User Agreement" was read and signed
ITEMS 1-20 ARE REQUIRED FOR ALL REQUEST TYPES		
21	SAAR	Select appropriate action for LAN, EMAIL, or VPN
22	UNIX	Enter user ID, Select Server; enter Folder if Datastage is needed
23	INFORMIX	Enter user ID, Database name, Environment (i.e. Production, Acceptance Test, Development)
24	DB2	Enter user ID, Database name, Environment (i.e. Production, Acceptance Test, Development)
25	SYBASE	Enter user ID, Database name, Environment (i.e. Production, Acceptance Test, Development)
26	SQL	Enter user ID, Database name, Server name
27	Direct Connect	Select if needed for DB2, enter Transaction Group
28	Access Level	Select level of access for UNIX, DB2, SQL
29	CVS	Enter FULL path of CVS database
30	VSS	Visual Source Safe, enter Server name and Folder names
31	SCOP2 (FMS)	Enter NITC mainframe user id
32	SYSTEM36	Enter system name needed
33	NITC	Enter user ID, select TSO level, CORE (list regions in "OTHER"), TRMS if needed
34	GLS	Enter NITC user ID, Type (i.e. District, EFT...)
35	ADPS	Enter user ID, Select Production or Development
36	PFCS	Select Level, enter your Approver. Responsibility, choose GL and/or BE and Type. Select range of Budget Levels
37	NFC	Enter user id, POI and ORG code(s), Agency. Select all applicable sub-systems
38	EAS	Enter e-Auth user ID OIP code(s), Role names
39	ISSO Initials	FOR FSA Security Office USE ONLY
40	Supervisor Initials	REQUIRED , supervisor must initial they have reviewed Page 1
41	Security Tracking No.	FOR FSA Security Office USE ONLY
42	CAIVRS	
43	HYPERION	Enter e-Auth user ID, NITC user id, District, S/Co Code, Environment, Database, Server, Group, and Role. Select required reports. MUST submit to Datamart Owner for Approval Prior to submitting to FSA Security.
44-46	IDMS Systems	Select at least 1 Database, Applicable User type(s) and ALL Applicable Group(s)
47	AS/400	Select User, Master, Communications or Other. If other, specify.
48	Other	Write in other access for above access, or if not specified above
49	Justification	Business justification for access
50A	Print Supervisor Name	Legibly print supervisor name
50B	Phone No.	Supervisor phone number
50C	Supervisor Signature	Signature of supervisor (Branch Chief or above)
50D	Date	Date signed by supervisor
51A	ISSO/SLR Signature	FOR FSA Security Office USE ONLY
51B	Date	FOR FSA Security Office USE ONLY
52	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		