Approval for FISRF – FS-6500-214, Forest Service, Albuquerque Service Center
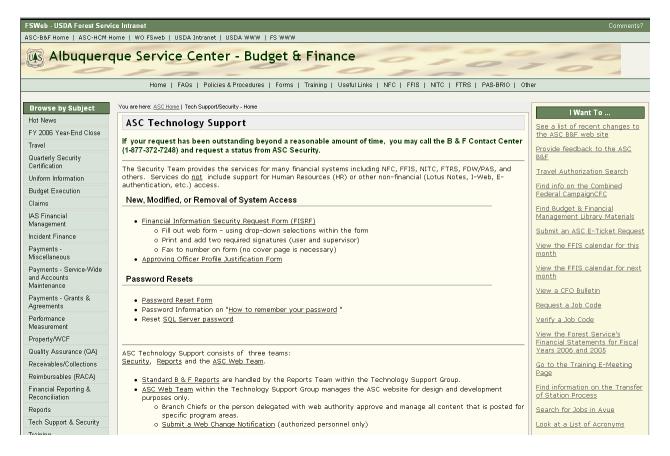
This form 6500-214 appears on the FSWEB for the ASC under Financial Information Security Request Form (FISRF) at this URL: http://fsweb.r3.fs.fed.us/asc/bfm/programs/technical-support/.

FSWeb - USDA Forest Service Intranet   Comments?
ASC-B&F Home | ASC-HCM Home | WO FSweb | USDA Intranet | USDA WWW | FS WWW

Albuquerque Service Center - Budget & Finance

Home | FAQs | Policies & Procedures | Forms | Training | Useful Links | NFC | FFIS | NITC | FTRS | PAS-BRIO | Other

Browse by Subject

You are here: ASC Home | Tech Support/Security - Home

- Hot News
- FY 2006 Year-End Close
- Travel
- Quarterly Security Certification
- Uniform Information
- Budget Execution
- Claims
- IAS Financial Management
- Incident Finance
- Payments - Miscellaneous
- Payments - Service-Wide and Accounts Maintenance
- Payments - Grants & Agreements
- Performance Measurement
- Property/WCF
- Quality Assurance (QA)
- Receivables/Collections
- Reimbursables (RACA)
- Financial Reporting & Reconciliation
- Reports
- Tech Support & Security
- Training

ASC Technology Support

If your request has been outstanding beyond a reasonable amount of time, you may call the B & F Contact Center (1-877-372-7248) and request a status from ASC Security.

The Security Team provides the services for many financial systems including NFC, FFIS, NITC, FTRS, FDW/PAS, and others. Services do <u>not</u> include support for Human Resources (HR) or other non-financial (Lotus Notes, I-Web, E-authentication, etc.) access.

New, Modified, or Removal of System Access

- Financial Information Security Request Form (FISRF)
  - Fill out web form – using drop-down selections within the form
  - Print and add two required signatures (user and supervisor)
  - Fax to number on form (no cover page is necessary)
- Approving Officer Profile Justification Form

Password Resets

- Password Reset Form
- Password Information on "How to remember your password "
- Reset SQL Server password

ASC Technology Support consists of three teams:
Security, Reports and the ASC Web Team.

- Standard B & F Reports are handled by the Reports Team within the Technology Support Group.
- ASC Web Team within the Technology Support Group manages the ASC website for design and development purposes only.
  - Branch Chiefs or the person delegated with web authority approve and manage all content that is posted for specific program areas.
  - Submit a Web Change Notification (authorized personnel only)

I Want To ...

- See a list of recent changes to the ASC B&F web site
- Provide feedback to the ASC B&F
- Travel Authorization Search
- Find info on the Combined Federal CampaignCFC
- Find Budget & Financial Management Library Materials
- Submit an ASC E-Ticket Request
- View the FFIS calendar for this month
- View the FFIS calendar for next month
- View a CFO Bulletin
- Request a Job Code
- Verify a Job Code
- View the Forest Service's Financial Statements for Fiscal Years 2006 and 2005
- Go to the Training E-Meeting Page
- Find information on the Transfer of Station Process
- Search for Jobs in Avue
- Look at a List of Acronyms

U. S. Forest Service

FS-6500-214 (Rev. 02/2007)
OMB 0546-NEW(Exp 08/2007)

Financial Information Security Request Form

Introduction

Welcome to the USFS Financial Information Security Request Form. On the next few screens you will be tasked with completing information needed by the Albuquerque Service Center - Budget & Finance IT Security Team. This information is necessary so that the IT Security Team can process your request quickly and completely.

Each screen you'll need to complete will contain navigation buttons at the bottom. Don't try to skip ahead since subsequent screens often depend on information from a previous screen. In most cases you can safely navigate backwards, though, if you need to double-check or modify entries you've already made.

Before you can proceed we must ask you to answer a couple of questions. Since certain training is required to access financial and Privacy Act-protected information, your responses to these questions will determine whether or not you may continue with this request.

Have you successfully completed IT Security Training within the past year?
○ Yes ○ No

Have you successfully completed Privacy Act Basics Training within the past year?
○ Yes ○ No

[Next Page]

Approval for FISRF – FS-6500-214, Forest Service, Albuquerque Service Center

Financial Information Security Request Form

FAX this form to ASC at 1-866-342-3441
with "Security Access Request" in the title of the fax.

User's Profile

Please enter your Lotus Notes Shortname, if you have one: [   ] **Please change incorrect data.**

Name: [ ]	Date of Request: 2/1/2007
EMail: [ ]	Telephone: [ ]
Title: [ ]	

Agency, Region, Unit (i.e. 11, 13, 28):	Agency	Region/Station/Area	Unit
	11	(Please select one) ▼	(Please select one) ▼

☐ Federal Employee	Social Security Number: [ ]
☐ Non-Employee (i.e. contractor)	Please enter expiration date: [Select Year ▼] [Select Month ▼] [Select Date ▼]

[Previous Page] [Next Page]

Action Requested

System	Add	Modify/ Reinstate	Remove	NA	User ID (if current user)
NFC	○	○	○	⊙	[ ]
FFIS	○	○	○	⊙	[ ]
For **PAS-Brio**, user must access http://pas.fs.fed.us prior to submitting form					
PAS-BRIO	○	○	○	⊙	[ ]
NITC	○	○	○	⊙	[ ]
ASR	○	○	○	⊙	[ ]
FTRS Spending	○	○	○	⊙	N/A
FTRS Billing	○	○	○	⊙	[ ]
PeopleSoft	○	○	○	⊙	[ ]
ASC SQL Server	○	○	○	⊙	[ ]
MITS	○	○	○	⊙	[ ]
ACRWS	○	○	○	⊙	[ ]
CPAIS	○	○	○	⊙	[ ]
HEAT	○	○	○	⊙	[ ]
FPPS	○	○	○	⊙	[ ]
FPPS with Datamart	○	○	○	⊙	[ ]

[Previous Page] [Next Page]

If NFC chosen:

NFC Access Request
Complete this section if NFC Add or Modify was selected on page 2.

Financial Systems	Range of Access			Access Scope
	Agency	Region/Station/Area	Unit	
(Please select one) ▼	11	(Please select one) ▼	(Please select one) ▼	(Please select one) ▼

[Add NFC System Record]

[Previous Page] [Next Page]

Approval for FISRF – FS-6500-214, Forest Service, Albuquerque Service Center

If FFIS chosen:

FFIS Systems Access Request			
Complete this section if FFIS Add or Modify was selected on page 2.			
FFIS Applications	CICS Region	FFIS	Application
(Please select one) ▼			
Add FFIS Application Record			

Previous Page   Next Page

If PAS/BRIO chosen:

PAS/BRIO Access Request
Select a group if PAS/BRIO Add or Modify was selected on page 2.
Group
(Please select one) ▼

Previous Page   Next Page

If NITC chosen:

NITC Access Request		
Complete this section if NITC Add or Modify was selected on page 2.		
NITC Systems	Range of Access	
	Region/Station/Area	Unit
(Please select one) ▼	(Please select one) ▼	(Please select one) ▼

Add NITC System Receord

Previous Page   Next Page

If ASR or other options are chosen:

Please use the space below for special requests.

Previous Page   Next Page

If MITS chosen:

Approval for FISRF – FS-6500-214, Forest Service, Albuquerque Service Center

MITS Access Request
Select an access level if MITS Add or Modify was selected on page 2.
Access Level
(Please select one) ▾

Previous Page   Next Page

After choices are made from drop-down options:

Agreement	
The following statement must be read and signed by the individual being designated for access. I HEREBY acknowledge the following: I recognize that FFIS and all other NFC systems contain data concerning individuals and commericial entities which is private or sensitive in nature. I agree not to use the information in these systems for unauthorized purposes, including those that result in the intrusion of the privacy of an individual or a commercial entity, or the unwarranted disclosure of personal or proprietary information. I agree not to share my access ID and/or password with others. I agree not to alter data in any FFIS document or table, or data elements in any NFC information system, for purposes of personal benefit or those that could result in theft or misuse of public funds.	
Signature of Applicant:	Date:
User's Supervisor - I certify that the user has received security instructions for the systems and/or applications as indicated, and I approve his/her access to these systems and/or applications, and the associated profiles.	
Supervisor's Name: Donna M Carmical	Telephone:
Signature of Applicant's Supervisor:	Date:
Signature of Security Administrator:	Date:
Reset Form	

PRIVACY ACT NOTICE

In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of your Social Security Number is authorized by Executive Order 9397 of November 22, 1943 and 5 U.S.C. 301. The primary purpose of requesting the Social Security Number (SSN) is to properly identify the employee. Many employees have similar names and the furnishing of the SSN will enable USFS to identify authorized users of USDA's computer systems. The information will be used by offices and employees who have a need for the information in the performance of their official duties. The information will not be disclosed outside USDA. Disclosure of your SSN and other information is mandatory. Failure to provide the requested information will result in the denial of the requested computer access authority.

Previous Page   Next Page

FINANCIAL INFORMATION SYSTEMS KEY SECURITY RULES

1. **DO NOT ACCESS**, research, or change any account, file, record or application not required to perform your official duties. You are forbidden to access your own account, that of a spouse, relative, friend, neighbor, or any account in which you have a personal or financial interest. If you are assigned to work on one of these accounts contact your supervisor. Behave in an ethical, technically proficient, informed, and trustworthy manner.

2. If you are asked by another person to access an account or other sensitive or private information, **VERIFY** that the requested access is authorized. You will be held responsible if the access is not authorized. As a general rule, you should not use a computer or terminal in behalf of another person.

3. **DIFFERENTIATE TASKS AND FUNCTIONS** to ensure that no one person has sole access to or control over important resources.

4. **PROTECT YOUR PASSWORD** from disclosure. You are responsible for any computer activity associated with your password. **DO NOT SHARE** your password with others or reveal it to anyone, regardless of his/her position in or outside the U.S. Forest Service. **DO NOT POST** your password in your work area. **DO NOT USE** another person's password. USER Ids must be treated with the same care as your password. Everything done with your user ID or password will be recorded as being done by you. Use unique passwords for each system and application you access. **NEVER** give your password out over the telephone. Be alert to others who may try to obtain your password. Social engineering is a practice used when hackers pose as system administrators. A hacker may randomly call a user and say that something is wrong on the system to get arbitrary access to your system. They may tell you that they need your password in order to issue new one. Always remember that system administrators DO NOT need your password in order to issue you a new password. Do not re-cycle passwords by using just a few over and over again, or make minor changes to passwords by adding a number to the base password.

5. **CHANGE YOUR PASSWORD** if you think your password is known by someone else. Immediately notify your supervisor or your Functional Security Coordinator or Security Representative. Passwords for PAS will be maintained in accordance with Forest Service Manual (FSM) 6684. Passwords shall:

a. Be changed or expire in 180 days or less.
b. Contain at least eight characters, a combination of alphabetic, numeric, and special characters,.
c. NOT contain: Any dictionary word in any language; any proper noun or the name of any person, pet, child, or fictional character; any employee number, SSN, birth date, phone number, or any information that could be readily guessed about the creator of the password; any simple pattern of letters or numbers, such as "qwerty", or "xyz123;" Any word, noun, or name spelled backwards or appended with a single digit or with a two-digit "year" string, such as 98xyz123

6. **DO NOT PROGRAM** your login or password into automatic script routines or programs.

7. **LOG OFF/SIGN OFF** or close the browser window for server based applications if you go to lunch, or break, or anytime you leave your computer or terminal. This is in addition to locking the workstation.

8. **PROTECT** your system against viruses and similar malicious programs. Make certain that updates to desktop virus protection schemes are performed in a timely manner in accordance with vendor or system administration instructions.

9. **PARTICIPATE** in Forest Service wide annual security training as required and read and adhere to security information pertaining to the PAS system hardware and software.

10. **RETRIEVE ALL** hard copy printouts in a timely manner. If you cannot determine the originator or receiver of a printout, dispose of it in a burn waste container or shredder. Store hardcopy reports and storage media containing sensitive information in a locked room or cabinet.

11. **IDENTIFY ALL** sensitive applications or data that you will be placing on a system, and any equipment processing sensitive information to your supervisor, so that appropriate security measures can be implemented.

Approval for FISRF – FS-6500-214, Forest Service, Albuquerque Service Center

12. **DO NOT USE PERSONAL EQUIPMENT** or software for official business without your supervisor's written approval.

13. **DO NOT INSTALL OR USE UNAUTHORIZED SOFTWARE** on Forest Service equipment. Do not use freeware, shareware or public domain software on Forest Service computers, without your supervisor's permission and without scanning it for viruses. Comply with local office policy on the use of antiviral Software.

14. **OBSERVE ALL SOFTWARE LICENSE AGREEMENTS**. Do not violate Federal copyright laws.

15. **DO NOT MOVE EQUIPMENT** or exchange system components without authorization by the appropriate functions and manager's approval.

16. **PROTECT FOREST SERVICE COMPUTER EQUIPMENT** from hazards such as liquids, food, smoke, staples, paper clips, etc.

17. **PROTECT MAGNETIC MEDIA** from exposure to electrical currents, extreme temperatures, bending, fluids, smoke, etc. Ensure the magnetic media is secured based on the sensitivity of the information contained, and practice proper labeling procedures. BACK UP critical programs and data, and store in a safe place. Back ups should be performed as often as program and data sensitivity require. Erase sensitive data on storage media before reusing or disposing of the media.

18. **DO NOT DISCLOSE THE TELEPHONE NUMBER(S)** or procedure(s) which permit system access from a remote location.

19. **DO NOT SEND OR STORE** Government information on a commercial E-mail site.

20. **DO NOT USE** sensitive information for equipment or program test purposes. Vendors should be escorted and monitored while performing maintenance duties.

21. **DO NOT DISCLOSE** or discuss any USDA personnel or vendor related information with unauthorized individuals. The Privacy Act of 1974, 5 USC 552a, prohibits such disclosure. A person making a willful unauthorized disclosure of information covered by this act may be charged with a Misdemeanor and subject to a fine of up to $5,000.

22. **PROMPTLY REPORT** all security incidents to your supervisor and in accordance with you agency policy on reporting incidents. For example: unauthorized disclosure of information, computer viruses, theft of equipment, software or information, and deliberate alteration or destruction of data or equipment. **NEVER ASSUME** that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident is reported more than once.

23. **SEEK** assistance and challenge unescorted strangers in areas where the system is being used.

To continue this request to completion you must indicate your agreement to abide by these rules. Failure to indicate agreement will result in your request not being submitted.

I AGREE ○ Yes ○ No

Clicking the "Finish" button will cause the data from this Form to be entered into the ASC B&F IT Security database, an email to be sent to the ASC Security inbox informing IT Security that your request has been initiated, and the entire form to be displayed to you for printing. The format for printing assumes one inch margins. Please check the Page Setup in your browser before printing to insure the margins are set correctly.

[Previous] [Finish]

After the selections are made, the form is printed and the request signed, a one page printout is faxed to 1-866-342-3441. This one page printout reflects the request and the signatures of the employee/contractor and the supervisor granting approval for this access. The one page printout is only required due to lack of e-signature approval and for audit purposes. Otherwise, this is an electronic request.