



FPPS Security Training

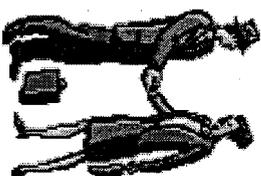
December 2003

Class Information

- **Instructors: Don Garcia**
Karlan Schneider
- **Class Times (approx):**
 - **Day 1: 8:30 – 4:00**
 - **Lunch: 11:30 – 12:30**
 - **Day 2: 8:30 – 3:00**
 - **Lunch: 11:30 – 12:30**

Introductions

- **Your Name**
- **Your Agency/Location**
- **Your FPPS Role/Experience**



Course Objectives

At the completion of this course, you will be able to:

- **Submit DSAF Requests**
- **Reset Passwords**
- **Add Offices**
- **Add Users**
- **Add Data Access**
- **Add Route Paths**
- **Establish Time and Attendance Security**

Course Information

- **Demonstrations**
- **Student Exercises**
- **Student Materials**
- **Class Assigned User ID/Password**

Student Logon & Password

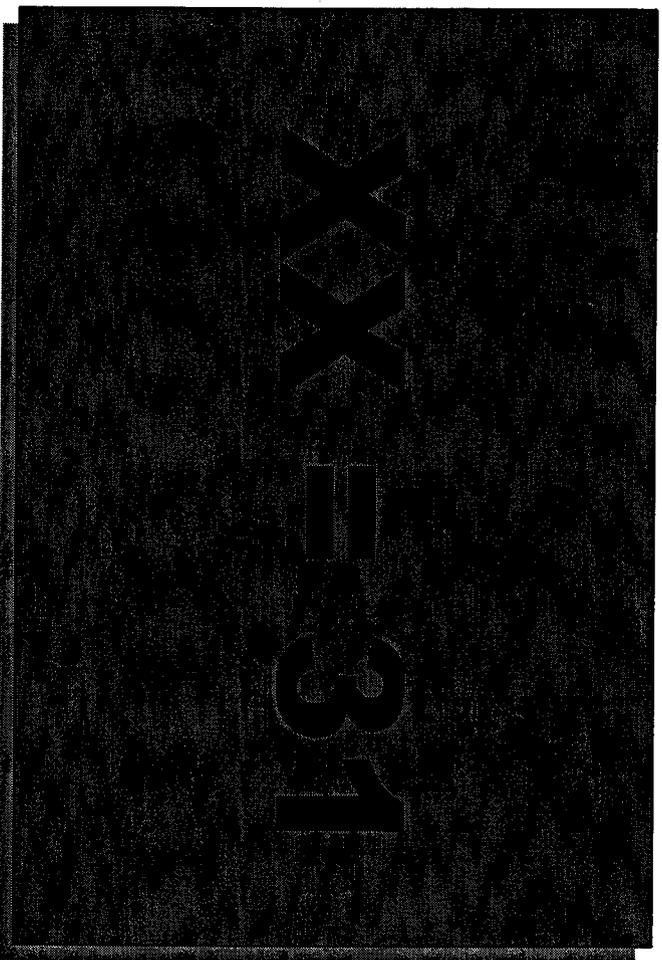
- Use class assigned User ID:

Jan Cooper

User ID: PPSJCXX

Student Logon & Password

- Use class assigned User ID: PPSJC31



Student Logon & Password

- **Use class assigned User ID:
PPSJCXX**
- **Your Password is:
den22nbc**
- **If your User ID is “REVOKED” during
class, inform the instructor**



FPPS Overview

FPPS is an online, integrated personnel/payroll system developed by the Department of the Interior's National Business Center (NBC), located in Denver, Colorado.

The system is used in the Federal Government for the processing of all personnel and pay-related functions. The system operates on an IBM mainframe computer in a database environment in which data is updated immediately.

Web FPPS Overview

Web FPPS allows you the convenience and flexibility of using the system at any time and at any place where you have access to the DOI intranet. Behind the scenes, the processes operate as they always have. However, with Web FPPS, you are able to take advantage of a windows-based environment using point-and-click technology.

Online Help

The Web FPPS Help System provides information about all end-user FPPS processes that are accessed via Web FPPS. Step-by-step instructions help you accomplish FPPS tasks such as SF52 transaction processing, employee and position maintenance, and security maintenance. The contents of the help system are current as of October 2003.



Online Help

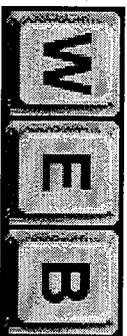
The WebFPPS Help System can be accessed at

www.nbc.gov

- Select FPPS from the Customer Express menu
- Click continue
- Click Online Help System

You may also go directly to WebFPPS at

webfpps.nbc.gov



Requesting Assistance

If you have questions about using FPPS, you may call the FPPS Help Desk. For SPOC related questions, call the NBC's Customer Service Center.

FPPS Help Desk

6:30 a.m. – 5:30 p.m. (MST/MDT)

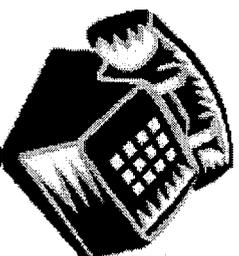
Phone: (303) 969-5500

FAX: (303) 969-5606 or (303) 969-7733

NBC Customer Service Center

24-hour telephone support

(303) 969-7777



Security Overview

- **Security controls within FPPS ensure that users are able to access only the records and processes for which they are responsible.**
- **FPPS security administrators are responsible for using the appropriate functions in the system to establish and maintain all end-user functions.**

Security Administrator Roles and Responsibilities

FPPS security administrators may perform one or more of the following roles:

- **Security Point of Contact (SPOC) - Responsible for establishing and maintaining user IDs and resetting user passwords that have been revoked**
- **FPPS Security Administrator - Responsible for establishing/maintaining offices, users-related authorities, and SF52 route paths**
- **T&A FPPS Security Administrator - Responsible for establishing and maintaining T&A offices and user-related authorities**

Types of Roles and Responsibilities Defined

Office types	User types	User responsibility
FPPS Top level administrative office located at the NBC	FPS - FPPS administrator (top level)	Maintain FPPS
	TBA - Tables administrator	Maintain FPPS tables
ADO Administrative office	ADM - FPPS administrator	Establish/maintain offices, user-related authorities, and SF52 route paths.
RO Requesting office	INI - Initiator	Initiate/maintain SF52 transactions (no signature authority)
	REQ - Requester	Initiate/maintain SF52 transactions (requester signature authority)
SPO Servicing personnel office	AUT - Authorizer	Initiate/maintain SF52 transactions (authorizer signature authority)
	AST - SPO assistant	Process SF52 transactions (no signature authority)
CVO Concurrenviewer office	SC1 - SPO signature authority	Process SF52 transactions (relational edit capability plus signature authority)
	SC2 - SPO legal approval	Sign for SF52 approval
TAC T&A corrections office	CON - Concurrer	View SF52 transactions (concurrer signature authority)
	VWR - Viewer	View SF52 transactions (no signature authority)
POD Payroll Operations Division (located at the NBC)	TAP - T&A processor	Process T&A corrections
	PAP - Payroll processor	Process payroll-related functions (no signature authority)
	PCR - Payroll certifier	Certify payroll schedules



Decentralized Security

Administration Facility (DSAF)

- The Decentralized Security Administration Facility (DSAF) is a specialized application of the CON-NECT electronic mail system on the IBM used only by Security Points of Contact (SPOCs). The DSAF cabinet is separate from any other CON-NECT cabinet. From DSAF, you cannot receive, send, or act upon mail in another cabinet.
- DSAF is used to electronically send an ASC-14 (Computer Center Access Request form) to the ADP security personnel at the National Business Center (NBC) in Denver, Colorado, to request access to the IBM computer system or to request that a user's current access be changed or deleted. This facility is also used to retrieve information sent back to you from the NBC regarding new user IDs and passwords or verification of a change or deletion.



Decentralized Security

Administration Facility (DSAF)

The NBC will answer all DSAF requests in a timely manner. Your request may be answered as quickly as the same day you submit the form, but no later than 3 working days after you submit the form.

Note: If you are a Webb FPPS system user, you must use the FPPS host screens for DSAF.



DSAFA Commands/Functions

- **ASC14** - Send a DSAFA request to the NBC's ADP Services Division staff. For detailed information, see Submitting an ASC14 Form.
- **V** - Access new verifications that have been sent to you. As soon as you display a verification, the system tags it as "old." You will be able to print verifications, if necessary.
- **O** - Access "old" verifications. Please note that old verifications will automatically be deleted after 90 days. You have the option to delete them yourself.
- **F** - Find an ASC14 that has previously been submitted. You will be prompted to enter a user's name, user ID, or SPOC user ID.
- **G** - Find a SPOC. You will be prompted to enter the SPOC's user ID.
- **E** - Exit DSAFA. You will see the FPPS screen.

Submitting an ASC-14 Form

- **Obtaining a user ID for a new IBM mainframe computer user is the most common reason to submit an ASC14 form.**
- **Other reasons to submit a form include deleting a user ID from access to the IBM or changing a user's access to one or more applications or processes.**

Submitting an ASC-14 Form

- **Agency** - Type the agency's 3-digit abbreviation (e.g., BOR, NPS, SSA, etc.) of the ID to be created
- **Name fields** - Type the user's last name, first name, and middle initial. For users with no middle name, leave a blank space in the MI field. (Note: Please verify that the user has no middle name. This prevents duplicate IDs.)
- **Category** - Type X for Civil Service or Contractor
- **Address/telephone** - Type city name, state abbreviation, and telephone number (including prefix)



Submitting an ASC-14 Form

- **Action requested** - Type X to select Add, Change, or Delete. (Note: For Change or Delete, provide the user's name and user ID. Also note that "delete" means removing the ID from the system. If access is to be removed from an application only, please specify in the special instructions.)
- **Access requested** - Type X to select the appropriate access
- **Special instructions** - Include instructions to explain any unusual circumstances; e.g., New SPOC only
needs password reset capability



Submitting an ASC-14 Form

Special instructions Note: Effective October 1, 2002, the Employee Health Benefits process was implemented in FPPS. Special access for the new command, FEHB, must be requested with a DSAF change request. This request must be documented in the Special Instructions field.



Interface Files

Security Points of Contact (SPOCs) are responsible for providing access to individuals within their respective organizations who need to access FPPS Interface File, Personnel and Payroll Report datasets on the IBM. Each client organization owns their own data and therefore is provided user-specific, high-level qualifier for datasets.

The IBM high level qualifier dataset naming convention for each client is established in concert with NBC staff. The client SPOC then obtains RACF user IDs to access the IBM mainframe through TSO and/or FTP. FPPS populates the datasets based upon set batch processing cycles (e.g., Biweekly, Monthly, etc.). Clients then schedule and access the datasets to move Interface File and Report data as input into their administrative applications for management and internal reporting purposes.

Password Reset/Revoke/Display

- **Security Points of Contact (SPOC) are responsible for resetting a user's access to the system when a user has been revoked by using the Password Reset process**
- **SPOCs may also use this process to deliberately revoke a user's access to the system or to display a user's current status**

Password Security

- **A password history retention disallows reuse of previous passwords**
- **User IDs will be revoked after 3 invalid password attempts**
- **User IDs will be revoked after 60 days of inactivity**
- **The maximum interval between required password changes for all clients in no more than 60 days**
- **Security Administrators will be set with a password change interval of 30 days**

Password Rules

- Passwords must be 8 characters in length
- The first and eighth position of the password must be a ALPHA character (A, B, C, etc.)
- The second through seventh positions of the password must contain a combination of both NUMERIC characters (1, 2, 3, etc.) and ALPHA characters (A, B, C, etc.)

Password Rules

You may use one of the three national characters in your password as follows:

- @ This special character may be used as an ALPHA character**
- \$ This special character may be used as an ALPHA character**
- # This special character may be used as an NUMERIC character**

Please note that these are the only special characters that the system will recognize

Office Maintenance

- **Through the Office Maintenance process, offices must be established in FPPS before users or route paths can be established**
- **Offices are defined by the appropriate department, bureau, subbureau, and organization codes**

Office Maintenance

- **Offices may be defined as one or more office types, depending on the function(s) performed by users within the office**
- **For example, an office may be defined as RO (Requesting Office), and SPO (Servicing Personnel Office), if there are RO users and SPO users functioning within the same office**

Office Types

- **Administrator Office**
- **Concurren/Viewer Office**
- **Requesting Office**
- **Servicing Personnel Office**
- **Payroll Office**
- **T&A Corrections Office**

Data Access Definition

- **Each FPPS office is defined to the system with at least one data access definition; i.e., a description of the department, bureau, subbureau, and organization code(s) for which users will have access authority**
- **Data access authority may be further defined by pay plan, grade or grade range, duty station code, and/or action type code**

Data Access Maintenance

- To access the data access definitions within your range of authority, you must use the OFFC, USER, or RPTH command
- Although there are three different commands used, any modification made to a data access definition using one command (e.g., OFFC) changes the definition system-wide
- You do not need to make the same modification using the other two commands



Adding Offices

- Offices must exist in the system before you can add users or route paths. Information required to add an office:
- The office ID of the new office (department, bureau, subbureau, and organization codes.)
- The POI and SPO location codes (only if the office is a SPO)
- The office types (determined by the user types in the office)
- One or more printer IDs (You can select printer IDs from a list once established)
- One or more data access definitions

ADP Division

ADP Division Office – 7211000

Bill Smith, Division Chief – REQ,AUT

Ken Pierce, Clerk – INI

System Software Branch – 721300

Sam Young, Branch Chief – REQ

System Support Branch – 721600

Shirley Newton, Branch Chief – REQ

ADP Division

ADP Division Office – 721000
Bill Smith, Division Chief
Ken Pierce, Clerk

The users in the ADP Division Office
will need data access to all their
organization codes

<u>Dep</u>	<u>Bur</u>	<u>Sub</u>	<u>Org Cd Min</u>	<u>Org Cd Max</u>	<u>PP</u>	<u>Gr</u>	<u>Dty Str</u>	<u>Act Typ</u>
IN	XX	01	721000	721600	*	*	*	*

ADP Division

Dep Bur Sub Org Cd Min Org Cd Max PP Gr Dty Stn Act Typ
IN XX 01 721300 (Blank) * * * *

The user in the System Software Branch will only need data access to their own organization code

System Software Branch – 721300
Sam Young, Branch Chief

ADP Division

Dep Bur Sub Org Cd Min Org Cd Max PP Gr Dty Stn Act Typ
 IN XX 01 721600 (Blank) * * * *

The user in the System Support Branch will only need data access to their own organization code

System Support Branch – 721600
 Shirley Newton, Branch Chief

ADP Division

ADP Division Office – 721000
 Bill Smith, Division Chief
 Ken Pierce, Clerk

IN XX 01 721000-721600 * * * * *
 IN XX 01 721300 * * * * *
 IN XX 01 721600 * * * * *

System Software Branch – 721300
 Sam Young, Branch Chief

System Support Branch – 721600
 Shirley Newton, Branch Chief

User Maintenance

- After offices have been established in FPPS, users may be established and maintained using the User Maintenance process
- The User List screen displays all offices within your authority listed by department, bureau, subbureau, and organization code
- Users within each office are listed alphabetically by last name

Adding New Users

After an office has been added to the system, you may add users to the office. You must know the user ID, title, SSN, and office ID of the new user.

Please note: When adding a new user, you may or may not see the User Maintenance screen. If the user is already defined to the system (e.g., as a T&A timekeeper), you will not need to complete the screen again when adding the user as an FPPS user.

Adding New Users

Required/Optional data on the User Maintenance screen:

- **LAST NAME** - protected; cannot be changed
- **FIRST NAME** - default-filled; may be changed
- **MIDDLE NAME** - optional
- **TITLE** - required; type any title
- **SSN** - required; type user's SSN directly over the zeros (no dashes)
- **DEPT, BUR, SUBBUR, ORG CODE** - type office ID
- **E-MAIL ADDRESS** - used for automatic e-mail notification when there are items (e.g., SF52s, Hold notifications, etc.) in the user's queue

Adding New Users

On the Command Selection window, you will select one (or more) office types. Subsequent screens will display the appropriate command selections for each office type, screen selections (for SPO users), signature authority selections, and data access definitions.

Route Path Maintenance

- **Through the Route Path Maintenance process, RO and SPO route paths create forwarding lists that are used to send SF52 transactions to other authorized system users**
- **SPO/RO route paths create forwarding lists that are used to send WGI notifications and probationary notices to managers for signature**
- **Sequencing the names on a route path puts the users' names in a specific order on the forwarding list**

Route Path Maintenance

All route paths are defined as:

- **Default or Qualified and**
- **RO, SPO, or SPO/RO**

Default Route Path

- A default route path encompasses all data access within the office
- There can only be one default route path per office

Qualified Route Path

- A qualified route path encompasses one or more specific data access(es) defined within the office
- The user's names that appear on the sequencing screen are those whose data access(es) are equal to or greater than the specific data access(es) selected as qualifying criteria for the route path

SPO and RO Route Paths

- **SPO - contains the user's names with SPO authorities that meet the data access criteria of the route path**
- **RO - contains the user's names with RO authorities that meet the data access criteria of the route path**

SPO/RO Route Path

- **SPO / RO route paths can only be created in a servicing personnel office**
- **SPO users' names are sequenced prior to RO users**
- **This type of route path accommodates distribution of automatically generated WGI notifications and probationary notices from the SPO to the RO**

T&A Input System Security

- **The Maintain T&A Security process is used to establish / maintain security controls for the FPPS T&A Input System**
- **To establish / maintain T&A security use the TSEC command**

T&A User Maintenance

For T&A user maintenance, you will assign:

- **Sequence Numbers (to indicate the order in which users' names will appear on forwarding lists)**
- **Signature Authority (timekeeper or certifier)**
- **Command Selections**