

## *FPPS Computer System Access Request Form*

I understand that when I use any of the National Business Center (NBC) Computer Systems and/or Automated Information Resources or gain access to any information therein, such use or access shall be limited to official Government business. Further, I understand that any use of the aforementioned systems or information that is not official Government business may result in disciplinary action consistent with the nature and scope of such activity. I have read the Rules of Behavior for FPPS. I understand them and agree to comply with them. I will report any violation of these rules to my supervisor.

FPPS Access requested:

New User                       Change/Update User                       Form Review/Recertification

Effective Date: \_\_\_\_\_ FPPS UserID (If current or former user) \_\_\_\_\_

\_\_\_\_\_  
Legal Name (Print or Type)

\_\_\_\_\_  
School/Location/Organization Code

\_\_\_\_\_  
Telephone Number

\_\_\_\_\_  
Social Security Number    XXX-XX-

\_\_\_\_\_  
Name of Supervisor/Manager (Print or Type)

\_\_\_\_\_  
Employee Signature                      Date

\_\_\_\_\_  
Signature of Supervisor/Manager                      Date

Permanent Employee                       Temporary Employee                       Contractor

|  |                                    |                                     |                 |
|--|------------------------------------|-------------------------------------|-----------------|
| Federal Personnel Payroll System (FPPS): |                                    |                                     | Org Code Range: |
| <input type="checkbox"/> Initiator       | <input type="checkbox"/> Requestor | <input type="checkbox"/> Authorizer | _____           |
| <input type="checkbox"/> View Only       |                                    |                                     | _____           |

Submit this completed form to your designated FPPS Security Point of Contact (SPOC):

Bureau of Indian Education (BIE)  
Edie Benson 505-563-5302  
Jacque Benavides 505-563-5313  
Fax: 505-563-5306

Bureau of Indian Affairs (BIA)  
Carl Cook 405-247-1655    Fax: 405-247-3920  
Mary Glory 405-247-1525    Fax: 405-247-3920  
Deb Abeita 505-563-5123    Fax: 505-563-5133  
Jack Kuntz 406-247-7956    Fax: 406-247-7902

|                      |                       |                      |                      |
|----------------------|-----------------------|----------------------|----------------------|
| For SPOC Use Only:   |                       |                      |                      |
| Form Received: _____ | DSAF Submitted: _____ | DSAF Returned: _____ | User Notified: _____ |
| FPPS User ID: _____  | USER: _____           | RPTH: _____          | WGI/PRB RPTH: _____  |

Solicitation of your Social Security Number (SSN) is authorized by Executive Order 9397, which requires agencies to use the SSN as the means for identifying individuals in personnel information systems. Your SSN will only be used to establish your access to FPPS. Furnishing your SSN is voluntary and failure to do so will have no effect on you. It should be noted, however, that where individuals decline to furnish their SSN, the SSN will be obtained from other records in order to complete registration.

### **User Confirmation and Certification of Compliance with the Rules of Behavior Regarding Access and Use of Federal Personnel Payroll Systems Data.**

I confirm that I have read, understand, and agree to abide by the requirements of the Rules of Behavior for the Federal Personnel Payroll System (FPPS) data to which I am seeking access.

Signed: \_\_\_\_\_ Dated: \_\_\_\_\_

## Rules of Behavior for Users of FPPS

The following Rules of Behavior (ROB) apply to all users of FPPS and must be reviewed by all users before granting them access to the Federal Personnel Payroll System (FPPS).

### 1. User Identification:

- A unique User ID is required for each individual FPPS user. User IDs must never be shared between users.
- User IDs possess privileges that are tailored to the duties of the individual user's job and to the individual user's level of "need-to-know." Each change in access must be made in writing using the attached form and approved by the user's supervisor. Completed forms are forwarded to the appropriate Security Point of Contact (SPOC) in the Human Resources Office (see attached form).
- If duties or job requirements change, accesses no longer needed must be removed and new accesses must be requested. Supervisors are responsible for notifying the SPOC whenever such changes occur so that the user's accesses can be changed to suit the new duty or job requirements.
- When employment terminates, for any reason, a user's access must be terminated. Supervisors are responsible for notifying the SPOC whenever a user leaves the organization, so that the user's access authorities can be removed. Under no circumstances may the logon account of a terminated user be given to another individual.

### 2. Passwords:

- Passwords are considered private and confidential. Users are prohibited from sharing their FPPS password(s). Attempting to enter an incorrect password three times will result in your user access being revoked. If you receive a message stating that you have been revoked, contact one of the SPOCs identified on the attached form.
- To minimize the risk of having the system compromised as a result of poor password selection; users are responsible for selecting passwords that are difficult to guess. FPPS users must follow these password guidelines:
  - Passwords must be eight characters exactly – no more, no less.
  - Passwords must begin and end with an alpha-character.
  - Passwords must contain at least one numeric character in positions 2 through 7.
  - New (changed) passwords may not be revisions of an old password. Reuse of the same password with a different prefix or suffix is not permitted.
  - Dictionary words, derivatives of User IDs, and common character sequences may not be used.
  - Personal details such as a spouse's name, license plates, social security numbers and birthdays should not be used unless accompanied by additional unrelated characters.
  - Proper names, geographical locations, common acronyms, and slang should not be used.
  - If exposed or compromised, passwords must be changed immediately.

### 3. General User Responsibilities

- Users are responsible for using the FPPS System and data for official business purposes only.
- Users of FPPS may not access, or attempt to access, data for which they are not authorized.
- Users are responsible for protecting the confidentiality of data associated with FPPS based on the sensitivity of the data. Such data may not be given to or shared with unauthorized persons.
- Users should report suspected or actual security violations to their supervisor or SPOC, and where appropriate, to the IT Security Personnel at their location.
- Casual browsing of sensitive or Privacy Act FPPS information, such as personnel data, is prohibited. FPPS users should only access FPPS data when there is an official business reason.
- Users are accountable for all actions associated with the use of their assigned FPPS User ID and may be held responsible for unauthorized actions found to be intentional, malicious, or negligent. Each user must protect his/her FPPS User ID by NEVER allowing another person to use or share his/her logon session. Because the logon session is directly associated with an individual User ID, the user is personally accountable for all actions performed with the User ID.

### 4. Consequences for Non-Compliance with these Rules of Behavior

The consequences of Federal employee or contractor behavior not consistent with these rules may result in revocation of access to FPPS, and wherever such actions may be applicable, disciplinary action consistent with the nature and scope of the infraction may be applied.