Minerals Management Service
Interim Policy Document

Effective Date: **May 4, 2006** **IPD No**. **06-06**
Series: Administrative
Title: Access and Review Procedures for the Federal Personnel/Payroll System and Quicktime

Originating Office: Human Resources Division, Administration and Budget

1. **Purpose.** To establish policy and standard procedures for the process of gaining authorized access to the Federal Personnel Payroll System (FPPS) or Quicktime. This Interim Policy Document (IPD) also establishes security review procedures for those user accesses.

2. **Objective.** To obtain documentation of authorization to access FPPS or Quicktime and to ensure access remains appropriate.

3. **Policy.** Every MMS employee or contractor who uses FPPS, Quicktime, or other HR systems where access is controlled by MMS must sign and submit the National Business Center (NBC) Computer System Access Request Form (Attachment 1), which includes the Roles and Responsibilities Statement, before receiving an ID and password to access the NBC FPPS or Quicktime programs. The employee's supervisor or the contractor's COTR must also sign the form. That access will be reviewed annually to ensure it is still appropriate.

4. **Authority.** Computer Security Act of 1987.

5. **Maintenance of Access Request Forms**.

A. **Access Request Forms**. The Access Request Forms must be forwarded to the appropriate Security Point of Contact (SPOC) for that organization. SPOCs are listed on the Access Request Form. When an employee or contractor leaves, the Access Request Form will be pulled from the active file, attached to the exit clearance form, and maintained in a secure, inactive file for 6 years, after which time it will be destroyed.

B. **Decentralized Security Administration Facility (DSAF) Requests**. NBC responses to requests made through the DSAF regarding new or modified user IDs must be printed and maintained with the user's Access Request Form in the office that initiated the DSAF request. DSAF requests to delete access upon termination of the employee or contractor will be maintained with the exit clearance form until its final disposition.

6. **Security Review**. A quarterly review of 25% of FPPS or Quicktime users (random sample) will be performed by the SPOC to verify accuracy of user roles and status. Sample used, findings, and correction action taken (if any) will be documented and

maintained with the Access Request Forms for one year. Inactive user ID's will be deleted after one year of inactivity.

7. **Cancellation**. This IPD will remain in effect until no longer needed or it is incorporated into the MMS Manual.

Robert E. Brown
Associate Director for
Administration and Budget

NBC Computer System Access Request Form

I, the undersigned, 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 the NBC Computer System and Related Resources provided to me. I understand them and I agree to comply with them. I will report any violation of these rules to my supervisor.

Access requested to the selected systems:

☐ FPPS ☐ T&A System ☐ Datamart

☐ Establish User Account ☐ Change User Account

Effective Date: _____ FPPS ID (If a current user): _____

_____ _____

Legal Name (Print or Type) Dept/Bureau/Office/Organization Code

_____ _____

Social Security Number Name of Supervisor / Manager (Print or Type)

_____ _____

Employee's Signature Date Signature of Supervisor / Manager Date

_____ _____

Employee's E-mail Address Employee's Telephone Number

☐ Permanent Employee ☐ Temporary Employee ☐ Contractor

Federal Personnel Payroll System (FPPS): **Org Code Range**

☐ Initiator ☐ Requester ☐ Authorizer ☐ Concurrer ☐ Viewer _____

☐ SPO ☐ Administrator

Time and Attendance System: **Org Code Range**

☐ Employee ☐ Timekeeper ☐ Certifier ☐ Administrator _____

Additional Instructions: _____

_____ _____

Individual Authorizing Dept.-Wide access (Print or Type) Signature of Authorizer Date

PLEASE return to your Employing Agency Security Point of Contact (SPOC)

Herndon (HQ) HR Systems Admin.
MMS - Mail Stop 2400
381 Elden Street
Herndon, VA 20170-4871
Fax: (703) 787-1046

SASC - Sarah Schlumbrecht
MMS - Mail Stop 2620
1201 Elmwood Park Blvd.
New Orleans, LA 70123
Fax: (504) 736-2478

WASC - Nanci Kodweis
MMS - Mail Stop 2720
P.O. Box 25165
Denver, CO 80225-0165
Fax: (303) 231-3929

For SPOC use only:
Date: DSAF Submitted: _____ Email Notification to user: _____

FPPS User ID: _____ QT User ID: _____ TSEC/QT: _____ USER: _____ RPTH: _____

Privacy Act Statement

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 the HR System. 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.

RULES OF BEHAVIOR FOR USERS OF COMPUTER SYSTEMS AND APPLICATIONS HOSTED AND MANAGED BY THE DEPARTMENT OF THE INTERIOR, NATIONAL BUSINESS CENTER

The following Rules of Behavior (ROB) apply to all users of applications and systems managed by the Department of the Interior (DOI), National Business Center (NBC). These ROB should be made available to all users before granting them access to an NBC-managed application system. They are intended to supplement any existing organizational ROB that might be in use.

1. User Identification

- A unique User ID is required for each individual user of an NBC-managed system or application. 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 approved.
- 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 whatever reason (e.g., death, medical leave of absence, retirement, termination for cause, etc.), 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

- Are considered private and confidential. Users are prohibited from sharing the password(s) for any NBC-managed system or application with anyone.
- 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. Wherever technically supported, as many as possible of the following password selection criteria should be employed:
  - Passwords must be at least eight characters in length.
  - Passwords should contain a mix of both upper and lower case letters, except for mainframe passwords, where case is irrelevant.
  - Mainframe passwords must contain at least one numeric character (0, 1, 2, 3...9) 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 (A, B, C, etc.) is not permitted.
  - Dictionary words, derivatives of User IDs, and common character sequences such as "123456" 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 NBC-managed computer systems and associated data for business purposes only.

- Users of NBC-managed systems and applications 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 the NBC-managed system or application to which they have been granted access, based on the sensitivity of the data. Such data may not be given to unauthorized persons.
- Users should report suspected or actual security violations to their supervisor or Security Point of Contact (SPOC), and where appropriate, to the application security administrator.
- **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. SPOCs

Security Points of Contact (SPOCs) are normally designated for each organization. Access to production data is approved and controlled by the data owner, through the SPOC for each application or system. SPOCs are responsible for:

- Approving and coordinating all requests for user access to the systems or applications they control.
- Complying with the SPOC ROB, which is completed during the SPOC assignment process and returned to the NBC IT Security Administration Office.
- Implementing controls to provide reasonable assurance that:
  - Physical and logical access to NBC-managed systems and applications, using computer terminals, is restricted to authorized users.
  - Audit reports of system use, made available by the NBC, are regularly reviewed.
  - Computer Security Incident Response procedures are in use at the user's site for reporting incidents involving or impacting NBC-managed systems and applications.
  - User access to NBC-managed systems and applications is properly authorized and assigned, and that segregation of duties is properly maintained.
- Reporting all suspected or actual security violations involving an NBC-managed system or application, to the NBC IT Security Administration Office.

5. Consequences for Non-Compliance with these ROB

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