Approved for Release
Deborah A. Jefferson
Director for Human Resources
Management

08/25/06
Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN # 043, FY06

SUBJECT: Access to the National Finance Center (NFC) Payroll/Personnel Processing System

EFFECTIVE DATE: Upon release of this HR Bulletin

EXPIRATION DATE: Effective until canceled or superseded

SUPERSEDES: N/A

BACKGROUND: Since October 7, 2003, the National Finance Center (NFC) has been administratively suspending user IDs that are inactive for 60 or more days. To avoid future suspensions, please be sure the users in your bureau/office are signing on regularly to the NFC Mainframe system.

PURPOSE: The purpose of this HR bulletin is to describe the procedures for requesting access to the NFC system for new users, requesting modifications to access for current users (including un-suspending "Asuspended" IDs), and deleting access for those who no longer need it.

PROCEDURES: Each Servicing HR Manager should designate a Security Access Coordinator (SAC) and an alternate, and provide this information to the Departmental NFC Security Officer. All requests for new access, modifications, Asuspended IDs, or deletions must be submitted by the SAC or the Servicing HR Manager to the Departmental NFC Security Officer. Requests for new access and modifications (except un-suspending passwords) must be approved by the Servicing HR Manager. Access requests will be completed within 7 to 10 days of receipt by the Departmental NFC Security Officer unless the NFC staff needs further information to fulfill the request. SACs are delegated authority to un-suspend and change passwords for their respective submitting offices without further approval.

1. Requests are to be submitted to the Departmental NFC Security Officer via e-mail addressed to Naccess@doc.gov. The specific information described below must be included in the request. Incomplete requests will be returned to the originator.

2. Requests to establish new User IDs may be submitted when an employee first becomes responsible for work in your office requiring access to the NFC Payroll/Personnel Processing System. User IDs may not be carried from one operating personnel office to another as in the case of a reassignment or transfer. [In such instances, the losing office must request that the User ID be deleted and the gaining office must request that a new User ID be established.] Requests for new User IDs may not be submitted before the new user is in the NFC database for the new position.

3. Requests must include the user's first and last name, and social security number (SSNO). If the individual is a contractor, indicate "CONTRACTOR" in place of the SSNO and provide an expiration date. Indicate what the NFC ID prefix should be (e.g., CSxxx (Census), NNxxx (NOAA), etc.). Request specific profiles or applications. Be sure that you provide clear instructions of the type of access needed, e.g., IRIS/Non-sensitive or IRIS/Sensitive, TMGT/Update. Include the Agency Number and Personnel Office Identifier (POI). SACs should review NFC's Procedures Manual for the systems needed.

4. Access to sensitive data in PINQ and IRIS must be specifically identified and should only be requested if the new user needs to see such data as Race/National Origin Code, performance rating, handicap code, etc., for individual employees. The "Range of Access" must indicate whether the new user needs access to all bureaus serviced by a given HR office (provide bureau numbers and POI number), to an entire bureau regardless of servicing personnel office (provide bureau number only), or to only that part of a bureau serviced by a given HR office (provide bureau number and POI). The "Access Scope" must indicate whether the new user should be permitted to look at records only or if the user is authorized to add or change records. If access to FOCUS is requested, the library (PWAFOCUS) to be accessed must be indicated.

5. Requests to modify a user's access must include the user's complete name, current NFC ID, Agency, and POI. If the individual is a "contractor," and has been extended, indicate the new expiration date. Specify profiles or applications to be deleted or added, as indicated above.

6. Requests to change passwords and un-suspend User IDs should be directed to the organization's SAC. If the organization's SAC or alternate is not available, the Departmental NFC Security Officer may provide this service.

7. When a user leaves an office or is assigned to duties which no longer require access to the NFC system, the SAC must suspend the User ID immediately, and submit a request to delete the User ID. The user's complete name and NFC ID must be provided.

8. When requesting access to the NFC Reporting Center, please supply the user's complete name, social security number, NFC ID (if the user has one), Agency/POI, e-mail address, type of reports (workforce, personnel actions or financial reports),

organization structure and data type (detail sensitive or non-sensitive). Reporting Center access can be limited to the lowest level of an organization.

9. HR Managers should have their SACs attend NFC Security Officer Training. Information on training can be found in the NFC training catalog at http://dab.nfc.usda.gov/supportcenter/tcatalog/01training/secg.htm#g1.

REFERENCES: SACs should review the NFC security procedures manual at http://dab.nfc.usda.gov/pubs/na-pubsmain.html. Individual Systems Procedure Manuals for specific security access can be reviewed at http://dab.nfc.usda.gov/pubs/na-pubsmain.html.

OFFICE OF POLICY AND PROGRAMS: Felicia Purifoy, Director, fpurifoy@doc.gov, (202) 482-5291

PROGRAM MANAGER CONTACT INFORMATION: Marie Waters, mwaters3@doc.gov, (202) 482-0056