for Will Ellmi

9-4-09

Approved for Release **Date**
Deborah A. Jefferson
Deputy Chief Human Capital Officer and
Director for Human Resources Management

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #109, FY09

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

EFFECTIVE DATE: Upon release of this HR Bulletin

EXPIRATION DATE: Effective until canceled or superseded

SUPERSEDES: Human Resources (HR) Bulletin #043, FY06

BACKGROUND: The National Finance Center (NFC) administratively suspends user IDs that are inactive for 60 days. To avoid suspensions, the users in your bureau/office will need to regularly sign on to the NFC Mainframe system and the NFC Reporting Center to ensure continuous access.

PURPOSE: The purpose of this HR bulletin is to provide the procedures for requesting access to the NFC system for new users, requesting modifications to access for current users (including un-suspending "Asuspended" identification (IDs)), deleting access for those who no longer need it, and adding the new parameters instructions for setting passwords for the NFC Mainframe system and the NFC Reporting Center.

PROCEDURES:

1. Each Servicing HR Manager should designate a Security Access Coordinator (SAC) and alternate, and this information should be provided to the Office of Human Resources Management (OHRM) NFC Security Officer via email at Naccess@doc.gov.
2. All requests for new access, modifications, Asuspended IDs, or deletions must be submitted by the SAC, or the Servicing HR Manager, to the OHRM NFC Security Officer.
3. NFC access requests will be completed within 7 to 10 days of receipt by the OHRM NFC Security Officer.
4. SACs are delegated authority to un-suspend and change passwords for their service population only without further approval.
5. All NFC systems access requests are to be submitted to the OHRM NFC Security Officer via e-mail addressed to Naccess@doc.gov.

Instructions for the most common NFC Systems Access Request:

1. New User ID - requests are submitted when an employee first becomes responsible for work in your operating unit, requiring access to the NFC Payroll/Personnel Processing System. User IDs may not be carried from one operating unit 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 be submitted before the new user is in the NFC database for the new position. SAC should contact the OHRM NFC Security Officer via telephone with the social security number (SSN) for the new user. Personal Identifiable Information, such as an employee's SSN, must not be sent via e-mail.
2. New Requests - must include the user's first and last name. If the individual is a contractor, indicate "CONTRACTOR" and provide a not to exceed date (NTE) for no longer than a year. At the end of the NTE date an extension can be requested. Indicate what the NFC ID prefix should be (e.g., CSxxx (Census), NNxxx (NOAA), etc.). Request specific profiles that apply to the job of the user by using the profiles for another user in the same position. The SAC must verify with the user's supervisor that the profile is acceptable for this position. Include the Agency Number and Personnel Office Identifier (POI).
3. Modification Requests - must include the user's complete name, current NFC ID, Agency, and POI. If the individual is a "CONTRACTOR," whose access needs to be extended, indicate the new expiration date, and specify profiles to be deleted or added to the user as applicable.
4. Suspended Mainframe Passwords - can be changed by the operating unit's SAC or alternate. If the operating unit's SAC or alternate are not available, the OHRM NFC Security Officer will provide this service.
5. Access Termination - When a user leaves an office or is assigned to duties that no longer require access to the NFC system, the SAC must suspend the user's access immediately, and submit a request to the OHRM NFC Security Officer to have the user's ID deleted. The user's complete name and NFC ID must be provided.
6. NFC Reporting Center Access Request - Submit the user's complete name, NFC ID (if the user has one), Agency/POI, e-mail address, type of reports (Workforce, Personnel Actions, Administrative or Financial Reports), organization structure and data type (detail sensitive or non-sensitive). For Financial and Administrative reports, you must specify which reports are required for the user. Reporting Center access can be limited to the lowest level of an organization.
7. Training requirements - It is strongly recommended that all SACs attend NFC Security Officer Training. Information on course description and availability can be found on the NFC home page under "Browse by Subject."

Parameters for setting NFC Mainframe Passwords: NFC has implemented changes to Top Secret password parameters. Top Secret is an application package that is used to secure mainframe resources. The new password changes will include the following:

1. Complex password enforcement - Passwords must contain at least one number; at least one letter (upper case or lower case); a special character of $, @, or #, which occurs between the first and last position. These are the only special characters allowed.

2. History of twenty-four (24) passwords - You cannot re-use a password with 24 changes, rather than the previous six (6).
3. Sixty (60) days maximum age limit of passwords - Passwords will expire every 60 days as opposed to the previous 90 days.
4. Five (5) failed login attempts - Passwords will be suspended after five failed login attempts, instead of the previous three (3).
5. Password length of eight (8) characters - Passwords must consist of exactly eight (8) characters instead of the previous six to eight characters.

NFC Reporting Center Password Policy Changes: The NFC Reporting Center password criteria have changed in compliance with A-123 security requirements for sensitive data protection and in preparation for upcoming security software enhancements. Upon expiration, passwords will have to be changed to conform to the new criteria which are at the 60 day interval. In order to be compliant with security mandates, passwords will be based on the following criteria:

1. Must be 12 characters.
2. Must contain the minimum of the following:
   1 Special character limited to: ! # $ % & * - +
   1 Westernized Arabic numeral (0-9)
   1 Upper case letter
   1 Lower case letter
3. You cannot re-use a password with 24 prior changes.
4. Maximum number of unsuccessful log in attempts is 5.
5. Maximum age of password is 60 days.

OFFICE OF POLICY AND PROGRAMS: Pamela Boyland, Director, pboyland@doc.gov, (202) 482-1068

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