Approved for Release
Kevin E. Mahoney
Director for Human Resources Management and
Chief Human Capital Officer

11/20/14
Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #195, FY15

SUBJECT: Guidance on the Procedures, Roles, and Responsibilities for Providing Access to the National Finance Center (NFC) system

EFFECTIVE DATE: Upon release of this HR Bulletin

SUPERSEDES: HR Bulletin #187, FY14, "Guidance on the procedures, roles, and responsibilities for providing access to the NFC system"

EXPIRATION DATE: Effective until superseded or revoked

PURPOSE: This bulletin provides guidance on the procedures, roles, and responsibilities for NFC Agency Security Officers (ASO), who are responsible for submitting and tracking NFC system access requests.

REVISION: This bulletin adds a section on Accountability, which clarifies the process used to validate the results of the mandatory, semiannual internal-review audits (the re-certification process); clarifies the procedures for conducting semiannual audits of users' access to the NFC system (to include specific measures on how to certify that the required audits were completed, and due dates to ensure they have been completed); and changes the schedule for performing the semiannual audits from the second and fourth quarters of the fiscal year (Q2 and Q4) to the first and third quarters (Q1 and Q3).

BACKGROUND: Each Servicing Human Resources Office (SHRO) is responsible for determining the NFC accesses needed for its serviced employees. Once determined, it is the responsibility of the SHRO to grant access to NFC as appropriate. To accomplish this, each SHRO must have at least one primary and one secondary NFC ASO who have the responsibility of submitting NFC system access requests to NFC through NFC's required procedures.

PROCEDURES: It is the responsibility of each SHRO to:

- Assign at least one primary and one secondary NFC ASO to ensure that security functions can continue if the primary NFC ASO is unavailable.

- Inform the NFC (via the NFC Remedy Requester Console) and the Department of Commerce (DOC) NFC Security Program Manager (via the NAccess@doc.gov mailbox) of any changes in ASO personnel. Notification must be provided within 5 business days of the change taking place. The DOC NFC Security Program Manager will keep a list of all active NFC ASOs.

It is the responsibility of ASOs to:

- Be educated on required ASO roles and access by completing training on the NFC Remedy Requester Console. The training is offered by the NFC, at no cost, via webinar and is held monthly. Details and specific dates can be found via: https://www.nfc.usda.gov/Security/Security_Training.html

- Forward a copy of ALL e-mails related to NFC security-access requests received from the NFC Remedy Requester Console, to the DOC NFC security main mailbox (NAccess@doc.gov). This is to ensure that reports can be generated for management upon request; ensure that auditor questions can be responded to timely and adequately; and to ensure that a record of all security-related correspondence with the NFC is kept in a central location.

- Conduct internal review audits (the re-certification process) semiannually at the conclusion of Q1 and Q3 of all NFC accesses currently in effect, to ensure that the level and scope of access above employee access is still valid and required, and resolve issues found during the audit.

  Note: This supplements NFC's monthly access reviews, which are not a substitute for ASO review.

- Convey **ALL** Personally Identifiable Information (PII), if required, to the NFC by following two methods:

  1. Via direct telephone interaction with the NFC security technician working on the access (no PII is to be left on voicemail) or
  2. Send securely through the DOC Accellion or other DOC-approved secure file transfer, to the following NFC mailbox: SELECTIVE.TEAM@nfc.usda.gov. In the body of the message, inform the Selective Team that the attached file contains information for the NFC security office; include the NFC Remedy Requester Console tracking number.

- Follow the NFC-published list of guidelines for ASOs, as follows:

  - Serve as the liaison between bureau/operating unit users and the NFC Access Management Branch.
  - Provide security awareness information to all employees upon their receiving an NFC user account, including providing rules of behavior, for example, informing employees that they are to keep their user accounts safe and to not divulge their passwords.

- Submit properly completed security access request forms via the Remedy Requester Console (https://servicecenter.nfc.usda.gov/arsys/home) listing user ID(s) and all required resources, level of access (Read or Update) needed, scope of access (organizational structure or Personnel Office Indicator) needed, and ensure PII data is encrypted. If the request is for a contractor, include the expiration date as well. The NFC has a standard set of forms (https://www.nfc.usda.gov/Security/Forms.html); however, SHROs can utilize their own forms if they prefer.
- Immediately suspend access to users who have separated, or as otherwise instructed, and submit a request to have the separated/specified employees' user account deleted via the Remedy Requester Console. To suspend Reporting Center access, change the users' password using the SecureAll (SALL) application.
- Review monthly security access reports to ensure that only authorized current employees have access to bureau/operating unit resources and to ensure that access for separated employees has been removed. To obtain security access reports for IRIS, PINQ, PMSO, or TINQ, run the "Payroll Personnel Access Report" within the Reporting Center. Otherwise, for other NFC applications, request the report from the NFC via the Remedy Requester Console. In addition, review (monthly) the ASO User ID list and Profile list reports.
- Refrain from requesting security access changes for one's own user ID.
- Provide proper justification for expedited security access requests. To expedite a request, ASOs must send an e-mail to NCCEscalation@nfc.usda.gov. Include the Remedy ticket number as well as a justification for the expedited request.
- Use access to provide only assigned, authorized functions.
- Call the NFC Operations and Security Center (OSC) to report access problems. OSC can be reached at 504-426-6435 or 800-767-9641, or via e-mail to osc.etix@nfc.usda.gov. Include the user's exact error message.
- Attend ASO training as needed.
- Attend quarterly ASO User Group meetings as needed.
- Remind those agency users whose accounts are about to expire (or be suspended) to logon and change their password.
- Remove password suspensions for their users. There are two types of suspensions: one is a "PSUSPEND," which is when an account is suspended for too many invalid logins. To remove a PSUSPEND, the ASO utilizes the "ASO" application on the NFC mainframe. The other type of suspension is an "ASUSPEND." This is when an account is suspended due to non-use. To remove an ASUSPEND, ASOs should submit an e-mail to osc.etix@nfc.usda.gov. (Note: ASUSPENDs should be examined for elimination.)
- Review and act upon security notifications.
- Use the SALL application to reset user passwords for FUND, FSDE, ITRS, OFEE, TUMS, IBIL, PADS, Reporting Center, and HIPS. ASOs should utilize the "ASO" application to reset mainframe passwords. For Insight password resets, send an e-mail to osc.etix@nfc.usda.gov.
- Review security access reports on the NFC Reporting Center to ensure that access for separated employees is removed.
- Update the NFC TMGT subsystem, Table 063, to reflect changes in authorized agency contacts.

ACCOUNTABILITY:

- SHROs are required to provide validation that they performed the required internal review audits (the re-certification process) by sending an e-mail to the NAccess@doc.gov mailbox. The validation must consist of a narrative explaining the results, which includes at a minimum:
    - Who performed the audits;
    - When they were performed;
    - What was audited: that is, a complete list of all supervisors and timekeepers who were checked; and the bureau(s)/Personnel Office Indicator(s) that were checked; and
    - A resolution of issues found must also be included in the validation narrative.

- Validation and results narrative must be completed by the 15th day after the end of the quarter (i.e., January 15 for Q1, and July 15 for Q3) or the next business day if the 15th falls on a non-business day to the NAccess@doc.gov mailbox.

- The DOC NFC Security Program Manager will review the validation submissions to ensure completeness and to look for systemic issues that need to be addressed DOC-wide or within a specific bureau/operating unit.

REFERENCES:

- NFC Security Officer Responsibilities: https://www.nfc.usda.gov/Security/Officer.html
- NFC Security Training: https://www.nfc.usda.gov/Security/Security_Training.html

OFFICE OF POLICY AND BENEFITS: OPBservices@doc.gov