/Kevin Mahoney/ 3/26/14

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

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #187, FY14

SUBJECT: Guidance on the procedures, roles, and responsibilities for providing access to National Finance Center (NFC) system

EFFECTIVE DATE: Upon release of this HR Bulletin

EXPIRATION DATE: Effective until superseded or revoked.

PURPOSE: This bulletin provides guidance on the procedures, roles, and responsibilities for ASOs, who are responsible for submitting and tracking NFC system access requests.

SUPERSEDES: None

BACKGROUND: Each Servicing Human Resources Office (SHRO) is responsible for determining the NFC accesses needed for its employees. Once determined, SHROs must have at least one primary and one secondary assigned NFC Agency Security Officer (ASO). Using NFC's required procedures, ASOs will have the responsibility of submitting NFC system access requests to the NFC.

PROCEDURES:

It is the responsibility of the SHROs to:

- Assign at least one primary and one secondary ASO, to ensure that security functions can continue if the primary 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@gov.com mailbox) of any changes in ASO personnel.

It is the responsibility of the SHROs' ASOs to:

- Be educated on ASO roles and access required 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 email 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 timely and adequately, and to ensure a record of all security related correspondence with the NFC is kept in a central location.

- Perform semi-annual (Q2 and Q4) internal audits of all NFC security accesses currently in force for areas of responsibility to ensure that the level and scope of access is still valid and required. Results of the review must be sent to the NAccess@doc.gov mailbox, and include the bureau(s)/POI(s) that was checked, along with a general overview of the findings. Any issues found are to be resolved via the NFC Remedy Requester Console. Note: This supplements NFC's monthly access reviews, which are not a substitute for ASO review.

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

    1. Via direct phone interaction with the NFC security technician working on the access (no PII is to be left on voice mail) 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 and include the Remedy Requester Console tracking number.

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

    - Serve as the liaison between agency users and the NFC Access Management Branch;
    - Provide security awareness information to all employees upon receipt of an NFC user account. This includes informing employees that they are to keep their user accounts safe and to not divulge their password;
    - Submit properly completed security access request forms via 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 (org structure or POI) needed, and ensuring 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 preferable;
    - Immediately suspend users access 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;

- Request and/or review monthly security access reports to ensure that only authorized current employees have access to agency 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, the ASO User ID list and Profile list reports are to be reviewed monthly;
- 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 email 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 email at 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 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 submit an email to osc.etix@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 email to osc.etix@nfc.usda.gov;
- Review security access reports on the NFC Reporting Center to ensure that access for separated employees is removed; and
- Update the NFC TMGT subsystem, Table 063, to reflect changes in authorized agency contacts.

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

PROGRAM MANAGER CONTACT INFORMATION: James Hoebel, JHoebel@doc.gov, 202-482-6372