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

11/19/14
Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #196, FY15

SUBJECT: Guidance on the Procedures, Roles, and Responsibilities for Providing Access to webTA

EFFECTIVE DATE: Upon release of this HR Bulletin

SUPERSEDES: HR Bulletin #188, FY14, "Guidance on the procedures, roles, and responsibilities for providing access to webTA"

EXPIRATION DATE: Effective until superseded or revoked

PURPOSE: This bulletin provides guidance on the procedures, roles, and responsibilities for those responsible for providing access to webTA.

REVISION: The 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 webTA (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 webTA accesses needed for its employees. Once determined, it is the responsibility of the SHRO (or designated personnel, such as timekeepers) to grant access to webTA as appropriate, including adding new employees to the webTA application to allow them to adequately process time and attendance. To accomplish this, each SHRO must have assigned at least one primary and one secondary webTA Security Officer or designated timekeeper. The designated personnel will have administrative access to webTA and be responsible for providing access to the webTA system.

PROCEDURES: It is the responsibility of the SHROs to:

- Assign at least one primary and one secondary webTA Security Officer (or timekeeper with responsibility for webTA administration) to ensure that security functions can continue if the primary webTA Security Officer or webTA Timekeeper is unavailable.

- Inform the Department of Commerce (DOC) webTA Security Program Manager (via the NAccess@gov.com mailbox) of any changes in personnel assigned to be webTA Security Officers/Timekeepers. Notification must be provided within 5 business days of the change taking place. The DOC webTA Security Program Manager will keep a list of all active webTA Security Officers, or designated timekeepers, performing that role.

It is the responsibility of the webTA Security Officers/Timekeepers to:

- Keep a record of all webTA accesses that they granted resulting from the SHRO's established enter-on-duty procedures.

- Ensure that webTA Timekeepers (and others who provide access to webTA) keep a record of who they provided system access to. Information to be recorded include: name, user ID, date access was granted, and the level of access. This record must be made available to the Office of Human Resources Management, auditors, and other authorized persons upon request.

  Note: Currently, webTA does not have access reporting within the system, thereby making this requirement a necessity. If/when an access report-generating capability has been added to webTA, this requirement will be re-examined, as authorized personnel will be able to obtain this information from webTA directly.

- Conduct internal review audits (re-certification process) semiannually at the conclusion of Q1 and Q3 of all webTA 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.

- Provide security awareness information to all employees who receive webTA user accounts, including providing and receiving signature on rules and behavior, which includes informing employees that they must keep their user accounts safe and not divulge their passwords.

- Ensure procedures are in place to immediately remove webTA access for users who have separated or transferred out of the security officers/designated timekeepers' area of responsibility; ensure that removal of access has been documented, and that the documentation has been retained.

- Refrain from making security-access changes for one's own user account.

- Provide access only for assigned and authorized functions.

- Ensure procedures are in place that allow for password resets and unlocking of accounts for users upon request.

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 webTA Security Program Manager will review the validation submissions to ensure completeness and to look for systemic issues that need to be addressed either DOC-wide or within a SHRO.

REFERENCES: Not applicable

OFFICE OF POLICY AND PROGRAMS: Valerie Smith, Director, vsmith@doc.gov, (202) 482-0272

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