3/26/14

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

Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #188, FY14

SUBJECT: Guidance on the procedures, roles, and responsibilities for providing access to webTA

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EXPIRATION DATE: Effective until superseded or revoked.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 those responsible for providing access to webTA.

SUPERSEDES: N/A

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 process time and attendance. To accomplish this, each bureau or SHRO must have at least one primary and one secondary assigned webTA Security Officer or designated timekeeper. The designated personnel will have administrative access to webTA and will have the responsibility of 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 who are assigned responsibility for webTA administration), to ensure that security functions can continue if the primary webTA security officer or 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 as the 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/designated timekeepers to:

- Keep a record of all webTA accesses that they granted resulting from the SHRO's established enter-on-duty procedure. In addition, ensure that Timekeepers (and others who provide access to webTA) keep a record of to whom they provided system access. Information to be recorded include: name, user ID, date access was granted, and level of access. This record must be made available to OHRM 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 capabilities has been added to webTA, this requirement will be re-examined as authorized personnel will be able to obtain this information from webTA directly;

- Perform internal review audits semi-annually (Q2 and Q4), of all webTA accesses currently in effect for areas of responsibility to ensure that the level and scope of access above employee access is still valid and required. Results of the reviews are to be maintained and made available to OHRM management, auditors, and other authorized persons upon request;

- Provide security awareness information to all employees upon receipt of a webTA user accounts and the Rules of Behavior (RoB) must be signed. This includes informing employees that they are to keep their user accounts safe and to not divulge their passwords;

- Ensure procedures are in place to immediately remove webTA user's access for users who have separated or transferred out of the security officer's/designated timekeeper's area of responsibility, that removal of access is documented, and documentation is retained;

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

- Provide access for only assigned, authorized functions; and

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

REFERENCES: Not applicable

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