JESSICA PALATKA

Digitally signed by JESSICA PALATKA
Date: 2023.08.17 06:44:11 -04'00'

Approved for Release
Jessica Palatka
Director, Office of Human Resources Management and
Chief Human Capital Officer

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #266, FY23

SUBJECT: Guidance on the Procedures, Roles, and Responsibilities for Providing Access to WebTA/GovTA and Conducting Periodic User Access Reviews.

EFFECTIVE DATE: Upon release of this HR Bulletin

SUPERSEDES: HR Bulletin #196, FY15, "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EXPIRATION DATE: Effective until superseded or revoked.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/GovTA or applicable timekeeping software system and conducting privileged user access reviews.

REVISION: The bulletin adds content regarding changes for privileged user re-certification processes that are applicable to customers of Enterprise Services. Specifically, ES has transitioned from a semi-annual privileged user audit to a real-time re-certification process that is driven by the privileged user and approved by a certifying official. SHROs may elect to transition to the real-time certification process utilized by ES and described here-in. Such a transition must be approved by, and coordinated with, OHRM

BACKGROUND: Each Servicing Human Resources Office (SHRO) and/or Enterprise Services (ES) is responsible for determining the timekeeping software accesses needed for its service population. Once determined, it is the responsibility of the SHRO/ES (or designated personnel, such as timekeepers) to grant access to timekeeping software as appropriate, including adding new employees to the application to allow them to adequately process time and attendance. To accomplish this, each SHRO/ES must have assigned at least one primary and one secondary timekeeping software Security Officer or designated timekeeper. The designated personnel will have administrative access and be responsible for providing access.

PROCEDURES: It is the responsibility of the SHRO/ES to:

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

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

active Security Officers, or designated timekeepers, performing that role.

It is the responsibility of the timekeeping software Security Officers/Timekeepers to:

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

- SHROs: Conduct internal review audits (re-certification process) semiannually at the conclusion of Q1 and Q3 of all 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.
  ES: Conduct a re-certification process for administrators, master supervisors, timekeepers, and master timekeepers (privileged users) every 180days. The privileged user will initiate the re-certification, which requires acknowledgement of the rules of behavior and be dependent upon approval from a certifying official (typically supervisor). The re-certification window (i.e., 180 days and based upon DOC policy) will be based upon the date access is initially granted or the most recent re-certification (whichever one is most recent). Privileged users will be notified of the need to be re-certify at 150 days. Privileged users will subsequently be notified every 2 weeks until re-certification is complete. If the re-certification is not complete (initiated and approved by the approving official) after 3 reminder notification (~192 days), the privileged access will be revoked.

- Provide security awareness information to all employees who receive timekeeping software 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 timekeeping software 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.

ES: Privileged users and approving officials will be conducting re-certification on a daily basis. ES will track and provide:

- Date of initial provisioning of privileged user access
- Date of most recent employee re-certification
- Name of the most recent certifying official
- Date of certifying official approval
- Date of de-provisioning (if applicable)

- SHROs: 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.
  ES: A listing of privileged users and their most recent re-certification will be provided at an interval determined by the WebTA/GovTA Security Program Manager

- The DOC timekeeping software 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/ES.

REFERENCES: Not applicable

OFFICE OF POLICY AND BENEFITS: OPBservices@doc.gov