Approved for Release
Deborah A. Jefferson
Director for Human Resources Management

June 16, 2007
Date

DEPARTMENT OF COMMERCE
OFFICE OF HUMAN RESOURCES MANAGEMENT

HUMAN RESOURCES (HR) BULLETIN #064, FY 07, (Title 5 U.S.C. § 552a)

SUBJECT: Rules of Behavior for WebTA

EFFECTIVE DATE: Effective immediately

EXPIRATION DATE: Effective until canceled or superseded

BACKGROUND: The Department's time and attendance (T&A) system, webTA, is a web-based application which allows users to easily access their T&A data via the World Wide Web using a web browser. The webTA system contains Personally Identifiable Information[1] (PII) that requires protection from loss or misuse. Although the unauthorized use of webTA is restricted by user authentication, and appropriate security controls are in place to assure confidentiality and integrity, employees with access to PII must ensure that the data is protected and only used for authorized activities and in authorized on-site and off-site work locations.

PURPOSE: The purpose of this HR Bulletin is to provide updated Rules of Behavior (ROB) for webTA users who have access to PII data to ensure that Office of Human Resources Management (OHRM) Information Technology (IT) resources are used in an efficient, ethical, and lawful manner. This HR Bulletin establishes the deadline for bureaus to have all ROBs for applicable serviced clients completed.

COVERAGE: The provisions of this HR Bulletin apply to all employees designated as timekeepers (or timekeeper delegates), HR administrators, and/or administrators (or administrator delegates) in webTA.

POLICY: Employees with access to PII data, based on their role assignments in webTA, are to sign and date the webTA ROBs and comply with all applicable guidance regarding access and data security. In accordance with the ROBs, accessing webTA PII data may only be done under the following conditions:

- If the user is authorized, based on his/her role assignments in webTA, to access PII data in webTA.

[1] Personally Identifiable Information is information that can be readily used for identity theft and other fraudulent activities and includes, but is not limited to, financial and payroll information, home addresses, home telephone numbers, social security numbers, etc.

- If the access is from an off-site location, the laptop/computer used must be government-owned and protected by Safeboot.

Servicing Human Resources Offices (SHRO) are responsible for ensuring that all (1) serviced clients are provided with the webTA ROBs, (2) ROBs for affected employees are completed and returned to the SHRO by August 10, 2007, and (3) new employees with access to webTA PII data comply with the provisions of this HR Bulletin and the webTA ROBs.

REFERENCES: Title 5 U.S.C. § 552a, Department of Commerce, Office of the Chief Information Officer's *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005, Office of Management and Budget's Memorandum 06-16, *Protection of Sensitive Agency Information,* June 23, 2006.

OFFICE OF POLICY AND PROGRAMS: Sheila Fleishell, Acting Director, sfleishell@doc.gov (202) 482-0022

PROGRAM MANAGER CONTACT INFORMATION: Sheila Fleishell, Program Manager, sfleishell@doc.gov, (202) 482-0022

US Department of Commerce

Office of the Secretary
Office of Human Resources Management (OHRM)
WebTA

Rules of Behavior

June 2007

WebTA
Standards of Acceptable System Use and Account Approval

Notice to all System Users: These standards apply to all users of Office of Human Resources (OHRM) Information Technology (IT) resources and are intended to increase individual awareness and responsibility, and to ensure that all users utilize OHRM IT resources in an efficient, ethical, and lawful manner. Failure to abide by these rules may constitute grounds for termination of access privileges, administrative actions such as disciplinary actions, and/or criminal prosecution, if warranted. All users must read and acknowledge these standards to receive access to OHRM IT resources, to include the following specific provisions:

1. I will only use userIDs for which I am authorized and will not divulge my userID or account access procedures to any unauthorized user.
2. I consent to monitoring and security testing to ensure proper security procedures and appropriate usage are being observed for OHRM IT resources.
3. I recognize that I should notify the DOC Computer Incident Response Team (phone number 202-482-7878) of all reportable incidents of IT security (viruses, unauthorized access, theft, inappropriate use, etc.). A reportable incident is defined in the DOC *IT Security Program Policy* found at http://www.osec.doc.gov/cio/oipr/ITSec/DOC-IT-Security-Program-Policy.htm#Incident Response Capability.
4. When I no longer require access to OHRM IT resources, I will notify my immediate supervisor, and make no further attempt to access these resources.
5. I understand that passwords are required for accounts on DOC computers. I will manage my passwords in accordance with the DOC *Policy on Password Management* and any password policy in effect.
6. I will not attempt to access any Personally Identifiable Information (PII) data in the WebTA application for which I am not authorized based on my role assignment in WebTA
7. I am only authorized to access WebTA PII data from an off-site location if the laptop/computer is government owned and protected by Safeboot. I understand that I am not authorized to access WebTA PII data from any unprotected site location.

Approval of all Privileged User Accounts: I certify that I have been provided a copy of the *Standards of Acceptable System Use and Account Approval* and that I have a need for privileged access in the performance of my official job duties.

Printed User's Signature	*User's Signature*	*Date*

I authorize the Account. I certify that he/she has an official need for privileged access.

Printed Supervisor's Name	*Supervisor's Signature*	*Date*