

DEPARTMENT OF THE INTERIOR
Privacy Impact Assessment

March 23, 2010

Name of Project: WebTA

Bureau: Office of the Secretary

Project's Unique ID (Exhibit 300): 010-00-01-07-01-1245-24

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

A. CONTACT INFORMATION:

Departmental Privacy Office
Office of the Chief Information Officer
U.S. Department of the Interior
202-208-1605
DOI_Privacy@ios.doi.gov

B. SYSTEM APPLICATION/GENERAL INFORMATION:

Notes: WebTA is a time and attendance software application that is the property of Kronos, Inc. The application is hosted at NBC and offered to our clients, however all application changes are made through Kronos.

1) Does this system contain any personal information about individuals?

Yes. WebTA contains the following personal information about individuals:

- Social Security Number
 - Name
 - User ID
-

a. Is this information identifiable to the individual?

Yes. The information is identifiable to the individual.

b. Is the information about individual members of the public?

Some information, such as name and User ID may apply to contractors who perform time and attendance functions (i.e., timekeepers) however the contractors' time and attendance information is not entered or stored in the application.

c. Is the information about employees?

Yes. The information in webTA is about employees of the Federal Government.

2) What is the purpose of the system/application?

The purpose of webTA is to input, validate, and certify time and attendance data for transmission to FPPS (Federal Personnel and Payroll System.) WebTA permits employee entry of time and leave requests, as well as traditional timekeeper data entry. WebTA provides some standard reports, based on access authority.

2a) List all minor applications that are hosted on this system and covered under this privacy impact assessment:

There are no minor applications hosted on webTA.

3) What legal authority authorizes the purchase or development of this system/application?

The legal authority for webTA is defined in the Office of Management and Budget Circular A-127, Policies and Standards for Financial Management Systems. This Circular is issued pursuant to the Chief Financial Officers Act (CFOs Act) of 1990, P.L. 101-576 and the Federal Managers' Financial Integrity Act of 1982, P.L. 97-255 (31 U.S.C. 3512 et seq.); and 31 U.S.C. Chapter 11.

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Categories of individuals covered in webTA currently are employees of non-Interior bureaus/agencies.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The information in webTA is entered by the individual or taken from the FPPS application and other sources, as follows:

- The initial personnel information on each employee is provided from interface files from the FPPS application or entered on-line by the administrator.
- Employee information is updated by administrators and timekeepers.
- Time and attendance data, including cost structure information, is entered by employees or timekeepers based on employee work effort during a pay period.
- Employee leave and profile data is updated from interface files from the FPPS application.

b. What Federal agencies are providing data for use in the system?

The following entities are scheduled to use webTA beginning in FY2010:

- National Science Foundation
- Social Security Administration
- Overseas Private Investment Corporation
- Department of Education
- Federal Energy Regulatory Commission

Department of the Interior bureaus and/or other agencies may be added.

c. What Tribal, State and local agencies are providing data for use in the system?

No Tribal, State, or local agencies are providing data for use in webTA.

d. From what other third party sources will data be collected?

Data is not collected from any other third party source for webTA.

e. What information will be collected from the employee and the public?

Time and Attendance data is collected from the employee. Data from the general public is not collected.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOI records be verified for accuracy?

Data accuracy is verified by the receipt or non-receipt of time and attendance data through edits that enforce the time and attendance rules based on the employee profile.

b. How will data be checked for completeness?

Data is checked for completeness by:

- Editing personnel data to ensure that all required fields are populated.
-

- Validating that all active employees have time and attendance records for the current pay period.
- Monitoring all input files to ensure they have been received.
- Performing edits against each input file to ensure that the receipt matches the transmittal.
- Timekeeper and supervisor review and approval.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

WebTA data is current. User profile data is uploaded from FPPS nightly. Leave balances are uploaded from FPPS bi-weekly. Time and attendance data is validated to ensure that it is for the correct pay period.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Data elements are described in detail and documented in the following documents:

- Elements listed in the Kronos, Inc Data Dictionary

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

The use of the data is both relevant and necessary to process and report time and attendance data. This data is necessary to produce payroll for agencies who use webTA.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

WebTA will derive new leave balances. This information is uploaded to and maintained in FPPS.

3) Will the new data be placed in the individual's record?

Yes, the new data will be placed in the individual's payroll records.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No, the new data will not enable additional determinations.

5) How will the new data be verified for relevance and accuracy?

The data is verified through edits established to validate the data.

- 6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Data is not being consolidated in webTA.

- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

Not applicable

- 8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Users retrieve webTA data via the employee name or user ID.

- 9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

WebTA produces reports for use by employees, timekeepers, supervisors, and administrators. These reports are used to verify the correct cost structures, verify employees by role, provide status by user role, provide various audit reports, verify leave balances, and provide statements of historical T&A records. (History begins at the time of conversion.)

- 10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent).**

WebTA contains no voluntary information. An employee's ability to consent to a particular use is governed by the policies of the individual client organizations.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

- 1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

WebTA is operated at one site.

- 2) **What are the retention periods of data in this system?**

WebTA is covered under General Records Schedule (GRS) 2, "Payrolling and Pay Administration Records.

Time and attendance source records include any record upon which leave is based. NARA's General Records Schedule 2, item 6 indicates that records may be destroyed after a GAO audit or after 3 years, whichever is sooner. Items 7 and 8 indicate that records may be destroyed after a GAO audit or after 6 years, whichever is sooner.

- 3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Procedures for disposing of data are followed in accordance with approved NARA regulations. Disposition procedures are documented at <http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/>.

- 4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

There are no new uses of the technologies used to operate and maintain webTA.

- 5) How does the use of this technology affect public/employee privacy?**

Not applicable

- 6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

No

- 7) What kinds of information are collected as a function of the monitoring of individuals?**

Not applicable

- 8) What controls will be used to prevent unauthorized monitoring?**

Not applicable

- 9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Payroll, Attendance, Retirement, and Leave Records – Interior, Office of the Secretary – DOI 85

Each government agency using webTA is responsible for their own system of records notice covering the collection of data at their agency.

- 10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

The system is not being modified.

F. ACCESS TO DATA:

- 1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)**

NBC data access is required by staff including both government and contractor staff performing system maintenance. Within each client organization, an administrator determines the roles of each individual – employee, timekeeper, and/or supervisor. The administrator assigns employees to the timekeepers and supervisors, thus restricting their access to the assigned individuals. Administrators may also assign timekeeper roles to contractors, as determined by the individual client's needs.

- 2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Each client designates the role of administrator. The administrator decides who has access to the data by assigning specific roles to the individual on a "need-to-know" basis. Access criteria, procedures, controls, and responsibilities beyond those built into the application are determined and documented by each user agency. Kronos maintains documentation of webTA configuration settings and options.

- 3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

The organization's administrator defines the access for timekeepers and supervisors. In the case of the employees, access is limited to their respective records. NBC also restricts access to a client's instance via firewall, etc.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

Administrators review access authorities on an on-going basis.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

Yes, contractor personnel are involved with design, development, testing and implementation as well as maintenance and general support. Appropriate security and privacy clauses are contained in the contracts, such as the Privacy Act Notification (FAR 1452.224-1 and FAR 52.224-01) and security per DOI OCIO memo of August 18, 2004, "Information Technology Security Requests for Acquisition."

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

WebTA shares data with FPPS. WebTA uploads time and attendance to FPPS for payroll calculation. FPPS transfers personnel information to webTA to populate new employees in the application.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The interface is not applicable to members of the public. NBC is responsible for protecting privacy rights as the host of the webTA and FPPS applications.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

No other agency will share data or have access to the data in webTA.

9) How will the data be used by the other agency?

Not applicable

10) Who is responsible for assuring proper use of the data?

The clients' administrators are responsible for assuring proper use of the data.
