asdfasdfasdf

webTA
Privacy Impact Assessment (PIA)

November 19, 2008

System Information

Name of System, Project or Program: webTA
OMB Unique Identifier: 015-35-01-01-01-1126-04

Contact Information

1. **Who is the person completing this document?**

   Patrick Greer
   Manager, OIT/DTS
   Bureau of the Public Debt
   200 Third Street, Room 202
   304-480-6205
   Patrick.Greer@bpd.treas.gov

2. **Who is the system owner (Authorizing Official)?**

   Carrie Roe
   Director, ARC/BTD
   Bureau of the Public Debt
   5th Floor Avery Street Building
   304 480-7230
   Carrie.Roe@bpd.treas.gov

3. **Who is the Information System Security Officer (ISSO)?**

   Patrick Greer
   Manager, OIT/DTS
   Bureau of the Public Debt
   200 Third Street, Room 202
   304-480-6205
   Patrick.Greer@bpd.treas.gov

4. **Who is the Information System Security Manager who reviewed this document?**

   Jim D. McLaughlin
   Manager, OIT/SAB
   Bureau of the Public Debt
   200 Third Street, Room 409
   Parkersburg, WV 26101
   304 480-7972
   Jim.McLaughlin@bpd.treas.gov

5. **Who is the Bureau Privacy Act Officer who reviewed this document?**

   Denise K. Nelson
   Privacy Officer, OMS/DAS/IMB
   Bureau of the Public Debt
   200 Third Street
   Parkersburg, WV 26101
   4th Floor Avery Street Building
   304 480-8402
   Denise.Nelson@bpd.treas.gov

6. **Who is the IT Reviewing Official (Chief Information Officer)?**

   Kimberly A. McCoy
   Assistant Commissioner (CIO), Office of Information Technology
   Bureau of the Public Debt
   200 Third Street
   Parkersburg, WV 26101
   304 480-6635
   Kim.McCoy@bpd.treas.gov

System Application/General Information

1. **Does this system contain any information in identifiable form?**

   Yes.

2. **What is the purpose of the system/application?**

   webTA is a web-based time and attendance (T&A) software application designed to capture hours worked, leave used, and accounting information on a biweekly basis. Public Debt, Administrative Resource Center (ARC) is a Shared Service Provider (SSP) and hosts webTA for Public Debt and franchise customers.

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

   webTA is an existing system, which received its Authority To Operate (ATO) in June 2004.

   Authority for maintenance of the system is permissible under 5 U.S.C. § 301; 31 U.S.C. § 321.

4. **Under which Privacy Act SORN does the system operate? (Provide the system name and unique system identifier.)**

   webTA operates under SORN Treasury/BPD.001, Human Resources and Administrative Records—Treasury/BPD.

Data in the System

1. **What categories of individuals are covered in the system?**

   Records cover present and former employees for Public Debt and franchise customers.

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?**

      Information is gathered from the individual, authorized timekeepers, supervisors, or uploaded from the National Finance Center.

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

      Federal payroll providers are providing data for use in webTA.

   c. **What State and/or local agencies are providing data for use in the system?**

      None.

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

      None.

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

No information is gathered from the general public. Personally Identifiable Information (PII), gathered on Federal employees, includes name and Social Security Number (SSN).

3. Accuracy, Timelines, and Reliability

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

PII within webTA is provided by the individual. Authorized ARC and other Federal agency employees enter this PII into the system.

ARC Relies on the individual, the individual's authorized timekeeper, or the Human Resources staff to update the information as appropriate.

b. How will the data be checked for completeness?

Data is checked for completeness by the data validation rules within webTA.

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.)

Yes, the data is current. ARC Relies on the individual, the individual's authorized timekeeper, or the Human Resources staff to update the information as appropriate.

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

Yes, the data elements are described in detail and well documented. Kronos produces a manual containing the data elements for webTA. The title of the publication is *webTA Data Guide For Report Writers*.

Attributes of the Data

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designated?**

   Yes, the use of the data is both relevant and necessary. The data is collected and maintained to ensure accurate and timely payment of salaries to Public Debt and franchise customer employees.

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?**

   No.

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

   Not applicable.

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

   No.

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

   New data is entered by employees and verified for relevance and accuracy by supervisors before record commitment.

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

   webTA has the ability to track individual actions within the application. The audit and accountability controls are based on Treasury and Public Debt policies and standards, which, in turn, are based on the applicable laws and regulations. These controls assist in detecting security violations, performance pRoBlems, and flaws in applications.

   Users are restricted to data that is only required in the performance of their duties (least privilege).

Additionally, the Department of the Treasury (Treasury), Public Debt (Public Debt) Information Technology (IT) Security Rules of Behavior ensure that users are made aware of their security responsibilities before accessing Public Debt's IT resources. All users are required to read and sign these rules acknowledging their responsibilities in protecting Public Debt's IT systems and data. Noncompliance with these rules may result in termination of access privileges, administrative actions, and/or criminal prosecution if warranted.

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

   Processes are not being consolidated; therefore, this question is 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 will be restricted to data that is only required in the performance of their duties. Only authorized personnel are able to run queries. Queries may be executed based on any data element within webTA. Kronos provides ARC with the *webTA Data Guide For Report Writers,* which identifies the data elements. The data elements are too numerous to list in this PIA.

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

   Reports, which query time and attendance data, can be generated from within webTA. Additionally, any data entered into webTA can be retrieved via Oracle Discoverer. However, user access to these reports is granted based on the separation of duties principle through assigned access authorizations and the least privilege principle.

   The reports generated using webTA data are used to compare and analyze time and attendance information and to resolve pay and leave errors.

   Each webTA user has access to standard reports within the system based on his/her level of access. Typical users (employees) can only generate reports containing their own time and attendance information. Timekeepers and supervisors can generate reports containing information for only those employees for which they are responsible. For reports generated outside the system using Discoverer, only personnel with a business need-to-know, as determined by the Human Resource Staff, are permitted access to these reports.

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?**

   The system is operated at only one location.

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

   Records are maintained in accordance with National Archives and Records Administration retention schedules.

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?**

   Paper and microform records ready for disposal are destroyed by shredding or maceration. Records in electronic media are electronically erased using accepted techniques.

   Reports are maintained in accordance with National Archives and Records Administration retention schedules.

   The Records Management Section is responsible for ensuring Public Debt's functions are adequately documented by ensuring permanent records are preserved, records no longer of current use are promptly destroyed, retention schedules are developed and implemented, and that Public Debt complies with the recordkeeping requirements issued by the Office of Management and Budget, the General Service Administration, the National Archives and Records Administration, and the National Institute of Standards and Technology. The procedures used to facilitate this process are documented on Public Debt's intranet.

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

   No.

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

   Data is consolidated and centralized within webTA. The employees' right to remain anonymous is protected and contingent upon the security controls implemented on the system and inherited from the Public Debt GSS (EITI).

These controls are checked for correct implementation and effectiveness at least annually through Public Debt's Certification and Accreditation process.

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

webTA does not have the ability to identify, locate, and monitor individuals. However, webTA has the ability to track individual actions within the application. The audit and accountability controls are based on Treasury and Public Debt policies and standards, which, in turn, are based on the applicable laws and regulations. These controls assist in detecting security violations, performance problems, and flaws in applications.

7. What kinds of information are collected as a function of the monitoring of individuals?

1. Date and time of access.
2. Subject identity (UserID or ProcessID).
3. Type of events (logon attempts and failures).
4. Information modified.
5. User account management (creation, deletion, and modification).
6. Actions by privileged users.
7. Event occurrence.

8. What controls will be used to prevent unauthorized monitoring?

Users are restricted to data that is only required in the performance of their duties (least privilege). The information system allows the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Additionally, Public Debt (Public Debt) IT Security Rules of Behavior (RoB) ensure that users are made aware of their security responsibilities before accessing Public Debt's IT resources. All users are required to read and sign these rules acknowledging their responsibilities in protecting Public Debt's IT systems and data. Noncompliance with these rules may result in termination of access privileges, administrative actions, and/or criminal prosecution if warranted.

9. Under which Privacy Act SORN does the system operate? Provide number and name.

webTA operates under SORN Treasury/BPD.001, Human Resources and Administrative Records—Treasury/BPD.

10. If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

The system is not being modified, therefore this is not applicable.

Access to Data

1. Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others.)

1. System Administrators.
2. Data Base Administrators.
3. webTA Support Staff.
4. End Users.

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

Access to data by a user is determined by the need-to-know requirements of the Privacy Act, the user's profile based on the user's job requirements, and managerial decisions.

Criteria, procedures, controls, and responsibilities regarding access are documented. The Department of the Treasury IT Security Program Directive 85-01 (TD P 85-01) clearly documents that the system manager is responsible for ensuring that access to the information and data is restricted to authorized personnel on a need-to-know basis. Additionally, PD F 5409-1 E, *Administrative Resource Center (ARC) System Access Form - End User Applications,* is used to request access to need-to-have applications. The PD F 5409-1 E is routed to appropriate managers for review and approval prior to access being granted.

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

Users will be restricted to data that is only required in the performance of their duties. The concept of "least privileged" is followed at Public Debt whereas the information system shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

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

Users will be restricted to data that is only required in the performance of their duties. The concept of "least privileged" is followed at Public Debt whereas the information system shall enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

webTA users are assigned a unique user id and password. User identifiers are managed by the following:

1. Verifying the identity of each user.
2. Receiving authorization to issue a user identifier from an appropriate organization official.
3. Ensuring that the user identifier is issued to the intended party.
4. Archiving user identifiers.

Users, logging into the webTA application, are presented with a sign-on screen requiring entry of a user name and password. The password characters are displayed as asterisks on the screen and are encrypted across the network. A user has three attempts to correctly enter their password before being denied access to the software. Once access has been gained, a list of the user's responsibilities is displayed.

IT Rules of Behavior have been provided to all franchise customers. Access Request forms must be submitted to ARC in order to obtain access to webTA. The franchise customer employee must sign the Access Request form stating that they have reviewed and understand the RoB.

RoB have been reviewed and signed by each Public Debt employee. The IT Security Rules of Behavior state that employees should:

1. Not read, alter, insert, copy, or delete any Public Debt data except in accordance with assigned job responsibilities. Ability to access data does not equate to authority to manipulate data. In particular, users must not browse or search Public Debt data except in the performance of authorized duties.
2. Notify their Supervisor when access to IT resources is no longer required, and make no further attempts to access the resources.

The above mentioned controls are used to prevent or discourage unauthorized use of the data. Audit features are in place and used to identify any

unauthorized use that has already taken place. These audit logs are only accessible by the webTA system administrators.

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, was Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?**

   webTA is a Commercial Off-The-Shelf product and is in the Operational and Maintenance Phase of the life cycle. No contractors are involved in the maintenance phase of the system.

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

   Yes, the National Finance Center (NFC) interfaces with webTA for such transactions as batch processes, file uploads, etc.

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

   Although all employees who have access to information in a Privacy Act system have the responsibility for protecting personal information covered by the Privacy Act, the information owner, system manager, and ultimately the Bureau CIO have the responsibility to see that the data is protected from all threats.

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

   Yes. Customer agencies will have access to the data in webTA. However, they are only permitted access to the data that pertains to their agency's personnel. Data is restricted to those employees of the agency with a business need-to-know. The reports provided to the agency are generated by Public Debt staff and distributed to appropriate agency contacts. Additionally, certain information is transmitted biweekly to NFC in order to generate salary payments.

9. **How will the data be used by the other agency?**

   The data would be used in a similar fashion as it is by Public Debt - to compare and analyze time and attendance information and resolve pay and leave errors.

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

Employees who have access to the system, the system manager, system owner and ultimately the Bureau CIO are responsible for assuring the proper use of data in the system.

The National Institute of Standards and Technology (NIST) requires Government organizations to establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

The Public Debt Disclosure Officer is responsible for administering requests for system data submitted to Public Debt involving the Privacy Act. Public Debt fully complies with the provisions of the Freedom of Information Act (FOIA), Title 5 U.S.C. Section 552, and the Privacy Act, Title 5 U.S.C Section 552a. Public Debt provides an established procedure to solicit requests to review and correct information recorded, and we have a dedicated Disclosure Officer who manages and administers the program.