The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):
https://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: **web Time and Attendance (webTA)**

Document Version: **Version 3.0**

Document Date: **06/07/2017**

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

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

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

Treasury/BPD.001, Human Resources and Administrative Records-Treasury/BPD.

3) If the system is being modified, will the SORN require amendment or revision?
__yes, explain.
_X_no

4) Does this system contain any personal information about individuals?
_X_yes
__no

a. Is the information about members of the public? No

b. Is the information about employees or contractors? Yes

5) What legal authority authorizes the purchase or development of this system?

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

DATA in the SYSTEM:

1) Identify the category of individuals in the system
Check all that apply:
_X_ Employees
__ Contractors
__ Taxpayers
__ Others (describe)

2) Identify the sources of information in the system
Check all that apply:

_X_ Employee
__ Public
__ Federal agencies
__ State and local agencies
__ Third party

a. What information will be collected from employees or contractors?

Name and Social Security Number.

b. What information will be collected from the public?

Not Applicable.

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

Federal payroll providers are providing data for use in webTA.

d. What state and local agencies are providing data for use in the system?

Not Applicable.

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

Not Applicable.

3) Accuracy, Timeliness, and Reliability

a. How are data collected from sources, other than Fiscal Service records, 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 data be checked for completeness?

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

c. What steps or procedures are taken to ensure 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. In what document(s) are the data elements described in detail?

The software provider, 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) How is the use of the data both relevant and necessary to the purpose for which the system is being designed?

The data is collected and maintained to ensure accurate and timely payment of salaries to Fiscal Service 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? How will this be maintained and filed?

No, the system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

No new data will be created.

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

No new data will be created.

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

No new data will be generated.

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 Fiscal Service 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 principle).

Additionally, the Department of Treasury (Treasury), Fiscal Service Information Technology (IT) Security Rules of Behavior ensure that users are made aware of their security responsibilities before accessing Fiscal Service's IT resources.

All users are required to read and sign these rules acknowledging their responsibilities in protecting Fiscal Service'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, not applicable.

8) **How will the data be retrieved? (If personal identifiers are used to retrieve information on the individual, explain and list the identifiers that will be used to retrieve data.)**

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. The software supplier provides ARC with the *webTA Data Guide for Report Writers*, which identify the data elements. The data elements are too numerous to list in this PIA.

9) **What kind 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 to access these reports.

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

Individuals do not have opportunities to decline to provide the information or to consent to particular uses of the information.

<u>MAINTENANCE AND ADMINISTRATIVE CONTROLS:</u>

1) **What are the retention periods of data in this system? How long will the reports produced be kept?**

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

2) **What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?**

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

The Records Management Section is responsible for ensuring the Fiscal Service 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 the Fiscal Service complies with the recordkeeping requirements issued by the Office of Management and Budget, the General Service Administration, the National Archives and Records Administration (NARA), and the National Institute of Standards and Technology. The procedures used to facilitate this process are documented on the Fiscal Service intranet.

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

The system is operated at only one location.

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

No, the system is not using technologies in ways that the Fiscal Service has not previously employed.

5) **How does the use of this technology affect employee or public 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 Fiscal Service GSS. These controls are checked for correct implementation and effectiveness at least annually through Fiscal Service's Security Assessment and Authorization (SA&A) 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 Fiscal Service 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 the applications.

7) **What kind of information is 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 principle). The information system allows the most restrictive set of rights/privileges or accesses needed by users (or process acting on behalf of users) for the performance of specified tasks.

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

ACCESS TO DATA:

1) Who will have access to the data in the system?
Check all that apply:

__ Contractors
_X_ Users
__ Managers
_X_ System Administrators
_X_ System Developers
__ Others (explain)_________

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 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 E *Administrative Resource Center (ARC) Online Application Access Request Form,* is used to request access to need-to-have applications. The PD F 5409 E is routed to request 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 for the performance of their duties. The concept of "least privileged" is followed at the Fiscal Service 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? (Please 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 the Fiscal Service whereas the information system shall enforce the most restrictive set of rights/privileges or accesses needed by users (or procedures 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 organizational official.
3. Ensuring that the user identifier is issued to the intended party.
4. Archiving user identifiers.

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 from stating that they have reviewed and understand the Rules of Behavior.

Rules of Behavior (RoB) have been reviewed and signed by each Fiscal Service employee. The IT Security Rules of Behavior state that employees should:

1. Not read, alter, insert, copy or delete any Fiscal Service data except in accordance with assigned job responsibilities. Ability to access data does no equate to authority to manipulate data. In particular, users must no browse or search Fiscal Service 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) **If contractors are/will be involved with the design, development or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?**

webTA is a Commercial Off-the-Shelf (COTS) 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?

_X_yes
__no

If yes,

a. Explain the interface.

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

b. Identify the role 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 responsibility for protecting personal information covered by the Privacy Act, the information owner, system manager and ultimately the Bureau CISO have the responsibility to see that the data is protected from all threats.

7) Will other agencies share data or have access to the data in this system?

_X_yes
__no

If yes,

a. Check all that apply:

_X_Federal
__State
__ Local
__Other (explain) ___________________

b. Explain how the data will be used by the other agencies.

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 the Fiscal Service staff and distributed to appropriate agency contacts. Additionally, certain information is transmitted biweekly to NFC in order to generate salary payments. The data would be used in a similar fashion as it is by Fiscal Service – to compare and analyze time and attendance information and resolve pay and leave errors.

c. Identify the role responsible for assuring proper use of the data.

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

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 agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

The Fiscal Service Disclosure Officer is responsible for administering requests for system data submitted to Fiscal Service involving the Privacy Act. Fiscal Service 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. Fiscal Service provides and established procedure to solicit requests to review and correct information recorded, and we have a dedicated Disclosure Officer who manages and administers the program.