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: moveLINQ

Document Version: 4.01

Document Date: May 30, 2017

SYSTEM GENERAL INFORMATION:

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

Information in this system of records is collected and maintained to enable Relocation Services Branch personnel and authorized Bureau of the Fiscal Service (Fiscal Service) personnel to process relocation travel documents for Permanent Change of Station (PCS) and Temporary Change of Station (TCS) moves for government employees in both Treasury and non-Treasury agencies.

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

BPD.001 – Human Resources and Administrative Records

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? Yes

b. Is the information about employees or contractors? Yes

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

5 U.S.C.301; 31 U.S.C.3101, et seq.

DATA in the SYSTEM:

1) Identify the category of individuals in the system
Check all that apply:

_X_ Employees
__ Contractors
__ Taxpayers
_X_ Others (describe) *Family members of relocating employees and seller/purchaser documentation associated with residence transactions.*

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

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

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

Information collected includes employee records relating to data required to create relocation obligations and payments. The employee provides documents as receipts for reimbursement, some of these documents concern transactions they have had with the public, for example real estate purchase/sale closing documents, which contain personal information on the public. Electronic images of these documents are stored within the moveLINQ application and can be retrieved by the applications users.

The system collects user authentication information provided by each user authorized to access the system. Users include Fiscal Service employees, relocating employee, and customer agency contacts.

The application has the following data fields available to store the values collected:

- Employee Name
- Authentication Information (User ID, Password)
- Employee Tax Identification Number (TIN)
- Employee Direct Deposit Information
- Employee Retirement Plan
- Employee Grade/Rank
- Employee Title (Current, New)
- Employee Current Home Address
- Employee Current Duty Station Address
- Employee New Home Address
- Employee New Duty Station Address
- Employee Phone Numbers (work, home, cell)
- Employee E-mail Address (work, personal)
- Employee Family – Names, Relationship, Birthdate
- Employee Salary Information
- Spouse Salary Information, if applicable.
- Employee Government Credit Card Number

Examples of information about the public furnished by the employee and contained on electronic images stored within the application:

Buyer/Seller Residence Transaction Information

- Name (both spouses)
- Current Address
- Property Address
- Purchase/Sale Price
- E-mail Address
- Phone Number
- Finance Company
- Loan Account Number
- Loan Information – Principle, payments, down payment, term, interest rate
- Insurance Company

Direct Deposit Information

- Name
- Bank Name
- Bank Routing and Transit Number
- Bank Account Type
- Bank Account Number
- Bank Address (Street, City, State, Zip)

b. What information will be collected from the public?

None

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

The following federal organizations provide data for moveLINQ:

Customers

- African Development Foundation
- Administrative Resource Center
- Alcohol/Tobacco Tax and Trade Bureau
- Armed Forces Retirement Home
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Bureau of the Fiscal Service
- Chemical Safety & Hazard Investigation Board
- Community Development Financial Institutions Fund
- Consumer Financial Protection Bureau
- Consumer Product Safety Commission
- Court of Appeals for Veterans Claims
- Department of Health and Human Services – ACF
- Department of Health and Human Services – ASA
- Department of Health and Human Services – ASPR
- Department of Health and Human Services - CDC

- Department of Health and Human Services - DAB
- Department of Health and Human Services - FDA
- Department of Health and Human Services – HRSA
- Department of Health and Human Services – HRQ
- Department of Health and Human Services – IEA
- Department of Health and Human Services – OASH
- Department of Health and Human Services – OCR
- Department of Health and Human Services – OIG
- Department of Health and Human Services – OMHA
- Department of Health and Human Services – ONC
- Department of Health and Human Services – OSG
- Department of Health and Human Services – PSC
- Department of Health and Human Services - SAMHSA
- Department of Homeland Security – CIS
- Department of Homeland Security – FEM (HQ)
- Department of Homeland Security – OIG
- Department of Homeland Security – ICE (No new activity after 10/10/2008)
- Department of Housing and Urban Development
- Departmental Offices – Department of the Treasury
- Farm Credit Administration
- Federal Housing Finance Agency
- Federal Housing Finance Agency – OIG
- Federal Maritime Commission
- Federal Mine Safety & Health Review Commission
- Financial Crimes Enforcement Network
- Library of Congress (No new relocations since 2/2009)
- Merit Systems Protection Board
- National Archives and Records Administration
- National Science Foundation
- Occupational Safety & Health Review Commission
- Office of Financial Stability
- Office of Government Ethics
- Office of the Comptroller of the Currency (No new relocations since 5/2009)
- Office of Thrift Supervision (Converted to Office of Comptroller of the Currency)
- Railroad Retirement Board
- Special Inspector General for Troubled Asset Relief Program
- Treasury Inspector General for Tax Administration
- Treasury Office of Inspector General
- TRICARE Management Activity
- United States Marshals Service
- United States Mint

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

None

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

Transportation service providers and relocation services companies under contract with our bureau are other third party sources.

3) Accuracy, Timeliness, and Reliability

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

Data collected from sources other than customer agency contacts/employees is verified for accuracy by bureau personnel. The relocating employee (Employee Type User) is able to review information as documents are prepared for them. They receive a copy of the Travel Order and participate in the vouchering review and approval process. The agency contact reviews information in the prepared documents as part of the review and approval process. The agency contact is also provided multiple reports presenting the information in different formats to be reviewed.

b. How will data be checked for completeness?

The system edits some fields to ensure the data has the correct type and number of characters and is in the correct format. Other fields are checked running an external audit report that highlights errors that need to be corrected prior to processing.

Questionnaires are completed by the customer agency employee who uploads them directly into the Employee Portal. The information is transferred into the System by Expense Management Type Users. Prepared information is shared with the customer agency employee to review for completeness and accuracy.

c. What steps or procedures are taken to ensure the data is current?

Data contained on the "Request for Employee Relocation" form is received directly from the customer agency contact. Data contained on the "Employee Questionnaire" and voucher forms are received directly from the customer agency employee. Data on these forms are reviewed by bureau personnel before populating the relocation.

Prepared information is shared with both the customer agency Employee Type User and Agency Contact User to review to ensure it is current.

d. In what document(s) are the data elements described in detail?

The vendor provides a data dictionary document with each release that has updates from the previous version. This is stored on the network with the release notes. It outlines field name, how the table data is stored and the format of the field and any audit checks performed by the application.

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?

Information in this system of records is collected and maintained to enable the Relocation Services Branch to create and process relocation travel documents, make payments and issue W-2 tax information.

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

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

N/A

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

N/A

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

N/A

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

Information is contained in secure buildings or in areas that are occupied either by officers and responsible employees of the Fiscal Service who are subject to personnel screening procedures and to the Treasury Department Code of Conduct or by agents of the Fiscal Service who are required to maintain proper control over records while in their custody. Additionally, since in most cases, numerous steps are involved in the retrieval process, unauthorized persons are unable to retrieve information in meaningful form. Information stored in electronic media is safeguarded by automatic data processing security procedures in addition to physical security measures. Moreover, for those categories of records stored in computers with online terminal access, the information cannot be accessed without proper credentials and preauthorized functional capability.

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

Yes. Security controls are reviewed annually. If the system undergoes a change that impacts security, a new security assessment and authorization would be completed.

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.)**

Data can be retrieved in a number of ways using a personal identifier. Information can be retrieved alphabetically by Employee ID (first 4 characters of the employee's first name plus the last four digits of the employee's SSN and a two-digit incremental counter), Employee Last Name, First Name, Relocation Document Number, Relocation Type Order Number, Old Duty Location (From), New Duty Location (To), Creator of the Relocation (Created By), Created On (Date), or by Relocation Date.

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

General activity reports, agency requested reports, and W-2 and tax filings. Authorized Fiscal Service personnel and customer agency personnel will have access and use these reports. The reports are used internally for tracking and processing obligations, amendments, vouchers, invoices, and tax filings.

Customer reports are typically used for recording and/or reconciling activity and billings, management reporting, status discussions, and support for agency data request responses.

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?**

The customer agency provides the Fiscal Service with a notice of an employee that is relocating; this notice will include contact information for the employee - name, phone numbers, and email address.

All employees complete forms that contain Personally Identifiable Information (PII) for themselves and their dependents. This information is necessary to calculate and properly reimburse them for expenses they incur as part of the relocation.

This PII information is supplied voluntarily by the employee. Fiscal Service answers all questions concerning the relocation including disclosing why Fiscal Service needs the information. The employee has the option to not disclose the information however it is explained to them how not providing the information would adversely affect the reimbursement of the expenses.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

   The retention period for all relocation travel records, forms, legal papers, and other related documentation is six years and three months from the date the relocation is closed.

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

   At the end of the retention period records are disposed of at varying intervals in accordance with records retention schedules reviewed, approved, and documented by the National Archives and Records Administration (NARA). Paper records ready for disposal are destroyed by shredding or maceration. Records in electronic media are electronically erased using accepted techniques.

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 only operated at one Fiscal Service site, a mirrored backup is maintained real time at a second Fiscal Service 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

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

   N/A

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

   Yes. Information in the moveLINQ system of records is collected and maintained to enable Fiscal Service to process relocation travel, make payments, and issue W-2 tax information.

7) **What kind of information is collected as a function of the monitoring of individuals?**

   Information collected includes residence, employment, address, email, fax, phone, and moving expense reimbursement information.

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

   Information is contained in secure buildings or in areas that are occupied by officers and responsible Fiscal Service employees who are subject to personnel screening procedures and to the Treasury Department Code of Conduct, or by agents of the Fiscal Service who are required to maintain proper control over records while in their custody.

Additionally, since in most cases, numerous steps are involved in the retrieval process, unauthorized persons would be unable to retrieve information in meaningful form. Information stored in electronic media is safeguarded by automatic data processing security procedures in addition to physical security measures. Moreover, for those categories of records stored in computers with online terminal access, the information cannot be accessed without proper credentials and preauthorized functional capability.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
   - **___ Contractors**
   - **_X_ Users**
   - **_X_ Managers**
   - **_X_ System Administrators**
   - **___ 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 the data by an Expense Management type user is determined by the Travel Service Division management.

   The type of access for each Expense Management type user is limited to what they need to perform their job function.

   The procedure for Travel Services Division (TSD) Expense Management user access is controlled through the moveLINQ Access Control Procedure. Access is requested by management. Access changes are logged in the moveLINQ Access Control Log. Access is controlled based on the role and the job functions performed by that role. Roles are reviewed annually as part of the Security Assessment. Each user's access and role is reviewed at least semi-annually.

   The procedure for Relocating Employee user access is controlled through the moveLINQ Access Control Procedure. Access is granted when a relocating employee (Employee Type User) has their first relocation created in the moveLINQ system. Access is not removed until all relocations for the relocating employee have expired and been deleted according to the record retention process.

   The procedure for the Agency Contact User's access is controlled through the moveLINQ Access Control Procedure. Access is granted when an authorized customer agency contact has provided the request for configuring the new user's access. The customer agency contact will review a list of Agency Contact Users annually. The list will contain all Agency Contact Users and a proposal to remove those users that have not accessed the moveLINQ system within a period of two years. The moveLINQ system administrators will remove any identified users from the moveLINQ system after the response deadline.

   Information is contained in secure buildings or in areas that are occupied either by officers

and responsible employees of Fiscal Service who are subject to personnel screening procedures and to the Treasury Department Code of Conduct or by agents of Fiscal Service who are required to maintain proper control over records while in their custody. Additionally, since in most cases, numerous steps are involved in the retrieval process, unauthorized persons are unable to retrieve information in meaningful form. Information stored in electronic media is safeguarded by automatic data processing security procedures in addition to physical security measures. Moreover, for those categories of records stored in computers with online terminal access, the information cannot be accessed without proper credentials and preauthorized functional capability. Fiscal Service maintains documented procedures concerning controls and responsibilities regarding access.

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

User access is restricted. Safeguards are in place to only allow users of the system to have access to the data they need to perform their job duties.

Only authorized travel personnel and database administrators will have direct access to the data. In addition, appropriate data will be provided to the following third parties:

- The Internal Revenue Services (IRS);
- The Social Security Administration (SSA);
- State Tax Departments;
- Third-party vendors for the transportation and storage of household goods and airline reservations;
- Home Sale Services vendors;
- General Services Administration (GSA); and
- Authorized customer agency personnel.

The Relocating Employee (Employee Type user) accesses the system through a limited use "Employee Portal" that displays only the information for that Relocating Employee that has been shared by the Expense Management users.

The Agency Contact User's access is restricted to their roles and responsibilities. The system will be configured to allow them to see only the information necessary to complete their duties as assigned.

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)**

Controls include continuous monitoring, rules of behavior, mandatory periodic training, and audit trails/logs.

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?**

N/A

6) **Do other systems share data or have access to the data in the system?**

_X_ yes
___ no

If yes,

a. Explain the interface.

Using a manual interface process the moveLINQ system interfaces accounting transaction data to the Fiscal Service core accounting system, Oracle e-Business Suite (OeBS).

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

The moveLINQ Authorizing Official is responsible for protecting the privacy rights of the public and employees affected by all approved interface processes from moveLINQ.

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
_X_ State
___ Local
___ Other (explain) _____

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

Only authorized personnel have access to the data in this system. Applicable tax data is provided to the Internal Revenue Service, Social Security Administration, and State Tax Departments. The General Services Administration and customer agencies personnel have indirect access to the data.

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

All Fiscal Service employees and contractors who have access to information in a Privacy Act system are responsible for protecting personal information covered by the Privacy Act.

The Relocating Employee will have access only to their own records. They will be personally responsible for protecting their own personal information.

The Agency Contact User's access will be restricted to only their assigned Relocating Employees as defined by their designated customer agency contact. The customer agency contact will be responsible for ensuring that these users have been properly vetted and trained to ensure they know how to control and properly use their Relocating Employee's personal information

covered by the Privacy Act.