



moveLINQ Privacy Impact Assessment (PIA)

September 1, 2007

System Information

Name of System, Project or Program: moveLINQ

OMB Unique Identifier: 015-35-01-02-1009-00

Contact Information

- 1. Who is the person completing this document? (Name, title, Organization, phone, e-mail, address).**

Lee Buckingham, Manager
Travel Services Division
Relocation Services Branch
304-480-8420
Lee.Buckingham@bpd.treas.gov
200 Third Street, Room A4-F
Parkersburg, WV 26106-1328

- 2. Who is the system owner? (Authorizing Official Name, title, organization, phone, email, address).**

Diana Bonnell, Director
Travel Services Division
304-480-5573
Diana.Bonnell@bpd.treas.gov
200 Third Street, Room A4-G
Parkersburg, WV 26106-1328

- 3. Who is the system manager? (Name, title, organization, phone, email, address).**

Lee Buckingham, Manager
Travel Services Division
Relocation Services Branch
304-480-8420
Lee.Buckingham@bpd.treas.gov
200 Third Street, Room A4-F
Parkersburg, WV 26106-1328

4. Who is the Information Systems Security Manager who reviewed this document? (ISSM Name, title, organization, phone, email, address).

Jim McLaughlin
Information Systems Security Manager
Division of Program Services
304-480-7972
Jim.McLaughlin@bpd.treas.gov
200 3rd Street, Room 409
Parkersburg, WV 26106-1328

5. Who is the Bureau Privacy Act Officer who reviewed this document? (Name, title, organization, phone, email, address).

Denise K. Hofmann
Disclosure Officer
Office of Management Services
304-480-8402
Denise.Hofmann@bpd.treas.gov
200 Third Street, Room A4-A
Parkersburg, WV 26106-1328

6. Who is the IT Reviewing Official? (CIO Name, title, organization, phone, email, address).

Kimberly A. McCoy
Assistant Commissioner
Office of Information Technology
304-480-6635
Kim.McCoy@bpd.treas.gov
200 Third Street, Room 302
Parkersburg, WV 26106-1328

System Application/General Information

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

Yes

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

Information in this system of records is collected and maintained to enable Relocation Services Branch personnel to process relocation travel documents for Permanent Change of Station (PCS) moves for government employees, both Treasury and Non-Treasury agencies.

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

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

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

BPD.001 – Human Resources and Administrative Records.

Data in the System

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

Present and former employees and immediate family members of our 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?

Individual

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

Refer to Relocation Services Branch Customer List, Attachment A.

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?

Employee Records relating to data required to create relocation obligations and payments.

- Employee Name
- Employee Tax Identification Number (TIN)
- Employee Retirement Plan
- Employee Current Home Address
- Employee Current Duty Station Address
- Employee New Home Address
- Employee New Duty Station Address
- Employee Phone Numbers
- Employee E-mail Address
- Employee Family – Names, Relationship, Birthdate
- Employee Salary Information
- Spouse Salary Information, if applicable

3. Accuracy, Timelines, and Reliability

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

N/A

- b. How will data be checked for completeness**

The system will edit each field to see that the data has the correct type and number of characters and is in the correct format.

- 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. Data received on the Request For Employee Relocation form is reviewed and verified to ensure data is current and not out-of-date.

- 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 the moveLINQ Standard Data Output Definitions document and in the moveLINQ Quick Reference Guide.

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, information in this system of records is collected and maintained to enable 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, and how will this be maintained and filed?**

Yes, data collected will be used to prepare and process relocation documents, schedule relocation travel for the employee and immediate family members, arrange for the transportation and storage of household goods, process real estate transactions, process tax payments and prepare W-2's. Data is stored on paper and in the moveLINQ system.

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

The data is placed in an existing employee's relocation file system with information on the individual.

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

Yes, new data will update an employee's record for an existing or new relocation.

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

The data is manually verified for relevance and accuracy. Out-of-date data is flagged and addressed immediately.

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

moveLINQ data is contained in secure buildings and processing environment. Employees of Public Debt are subject to the Treasury Department Code of Conduct and must undergo periodic personnel screening procedures.

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 would impact security, a new certification and accreditation would be completed.

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.

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, Relocation Document Number or by Relocation Date.

9. What kinds 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. RSB personnel and customer agency personnel will have access and use 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 maintained at the Bureau of the Public Debt's (BPD) facility and at the Bureau's off-site backup facility. BPD uses remote copy technology for data replication to our backup facility.

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

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

- 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?**

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.

- 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?**

Not applicable

- 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 ARC to process relocation travel, make payments and issue W-2 tax information.

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

Residence transaction information

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

Information is contained in secure buildings or in area which are occupied either by officers and responsible employees of Public Debt who are subject to personnel screening procedures and to the Treasury Department Code of Conduct or by agents of Public Debt 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 passwords and preauthorized functional capability.

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

BPD.001 – Human Resources and Administrative Records.

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

The existing Privacy Act system or records, which covers this system, was not substantially revised in FY06 and FY07.

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

RSB personnel
OIT Database Administrators

These records may be disclosed to:

- The Internal Revenue Services (IRS) and State Tax Departments for the purpose of processing tax withholdings.
- Third-party vendors for the transportation and storage of household goods and airline reservations
- Real Estate Sale Transactions

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

Information is contained in secure buildings or in area which are occupied either by officers and responsible employees of Public Debt who are subject to

personnel screening procedures and to the Treasury Department Code of Conduct or by agents of Public Debt 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 passwords and preauthorized functional capability. BPD 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.

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.)

Security Plan
Risk Management Plan
Certification and Accreditation Process
Roles and Permissions Security Matrix
Rules of Behavior
Mandatory periodic Training in Computer Security Awareness
Quarterly Newsletter "Frontline"
Audit Trails/Logs

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 statutory and regulatory measures addressed?

Yes, since the system is a Commercial off- the-Shelf (COTS) system, contractors are involved with the design and development. The system is maintained by BPD. The contractors do not have access to our data.

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

Yes. The moveLINQ system provides accounting transaction data to the Public Debt core accounting system, Oracle Federal Financials.

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

All BPD employees who have access to information in a Privacy Act system are responsible for protecting personal information covered by the Privacy Act. The information owner, system manager and ultimately the BPD 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)?

Only RSB personnel have access to the data in this system. Applicable tax data will be provided to the Internal Revenue Service, Social Security Administration and State Tax Departments.

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

For the purpose of administrating federal and state tax requirements.

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

All RSB 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 Public Debt Disclosure Officer is responsible for administering requests for system data submitted to the Bureau 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.

Attachment A

**Relocation Services Branch
Customer List**

Administrative Resource Center
Alcohol/Tobacco Tax and Trade Bureau
Armed Forces Retirement Home
Bureau of the Public Debt
Centers for Disease Control and Prevention
Chemical Safety & Hazard Investigation Board
Community Development Financial Institutions Fund
Court of Appeals for Veterans Claims
Department of Homeland Security – CIS and OIG
Departmental Offices
Farm Credit Administration
Federal Housing Finance Board
Federal Maritime Commission
Federal Mine Safety & Health Review Commission
Financial Crimes Enforcement Network
Financial Management Service
Franchise Business Activities
Library of Congress
Merit Systems Protection Board
National Archives and Records Administration
National Science Foundation
Occupational Safety & Health Review Commission
Office of Government Ethics
Office of Thrift Supervision
Railroad Retirement Board
Smithsonian Institution
Treasury Office of Inspector General
Treasury Inspector General for Tax Administration
United States Mint