EPA United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 07/2018)

Please submit your responses to your Liaison Privacy Official http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Brooks Patricia @ Brooks.patricia@epa.gov or (202) 564-3717

System Name: moveLINQ (mLINQS)	
Preparer: Eric Kim	**Office: OCFO/OB**
Date: 05/20/2019	**Phone: 202-564-6203**
Reason for Submittal: New PIA____ Revised PIA__X__ Annual Review____ Rescindment ____	

This system is in the following life cycle stage(s):

Definition □ Development/Acquisition □ Implementation □

Operation & Maintenance ☒ Rescindment/Decommissioned □

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

The moveLINQ Relocation Software (mLINQS) supports the EPA's Permanent Change of Station (PCS) travel relocation process as used by the Cincinnati Finance Center (CFC) Federal Employee Relocation Center (FERC) office.

We have an existing PIA on file. Just updating it to reflect the upcoming Cloud environment change.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

The SORN (EPA-29) documents the system's legal authority to collect, maintain and use privacy information. From EPA-29: Authority for Maintenance of the System: OMB Circular A–127; Chief Financial Officers Act of 1990, Public Law 101– 576; Federal Managers Financial Integrity Act of 1982, Public Law 97– 255 (31 U.S.C. 3512 et seq.); 31 U.S.C. Chapter 11.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes. The most recent ATO expires on June 30, 2021.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

ICR No. 0937.18; OMB No. 2030-0020.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

SaaS on the Microsoft Azure Government Cloud (Azure Virginia)

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

SSN, Name, Address, email address, Children's Name and DOB, Spouse's Name, Filing Status (for Tax Purposes).

2.2 What are the sources of the information and how is the information collected for the system?

The information is collected directly from the employee via a form.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

The data comes electronically directly from the employee – accuracy is maintained through directly coming from the source.   All information goes through a two-step process where one individual enters the data and a second individual confirms the data. This is called a quality audit check.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

Having the collected information: SSN, Name, Address, email address, Children's Name and DOB, Spouse's Name. There is a transmission risk from end user to the mLINQS application.

Mitigation:

Information is not shared with other systems. Information cannot be accessed remotely. We rely on mLINQ's and Azure Government to ensure safety of the transmissions of data.

Section 3.0 Access and Data Retention by the system

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes. mLINQS utilizes a role-based authorization strategy to provide the greatest level for administrative control and scalability by the Account Manager and/or Administrator. Access to operations within the mLINQS application is secured based on the role of the authenticated user provided by the Account Manager and/or Administrator. The role-based authorization can be fully configured by the Account Manager and/or Administrator based on EPA's requirements. This flexible design allows ERRC to create roles and apply permission or access rights to each function in the system. All users are subject to security controls and roles in the system. They all have at least a basic NACIS background screening. All EPA personnel with access to sensitive data and who are authorized to or able to bypass security controls, are required to undergo a higher level of background screening sponsored by EPA.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

mLINQS utilizes a role-based authorization strategy to provide the greatest level for administrative control and scalability by the Account Manager and/or Administrator. Access to operations within the mLINQS application is secured based on the role of the authenticated user provided by the Account Manager and/or Administrator. The role-based authorization can be fully configured by the Account Manager and/or Administrator based on EPA's requirements. This flexible design allows ERRC to create roles and apply permission or access rights to each function in the system. Access controls are documented in the mLINQ's SSP.

3.3 Are there other components with assigned roles and responsibilities within the system?

No

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

EPA federal employees.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Records are maintained for 6 years and 3 months after final payment. They are deleted when no longer needed. 1010

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

That there is a possibility of a data breach during the 6 years and 3 months**.**

Mitigation:

Data files are kept on secured servers at a secure site to minimize the risk of a breach.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party *private sector entities.*

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Yes. The tax information is shared with the IRS and state taxing authorities both electronically and manually (no direct interconnections). Outside entities do not have access to mLINQS.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

Tax information is shared with the IRS and state taxing authorities supporting the PCS relocation process

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

None

4.4 Does the agreement place limitations on re-dissemination?

None

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

That the taxing authorities don’t have the same level of security as the EPA. There is a risk of mail being sent to wrong address or becoming missing.

Mitigation:

The information is only provided to those taxing authorities that are required by law and the taxing authorities must assume the risk once the data is shared. mLINQS will send all documents containing sensitive material with tracking and signature confirmation or by registered mail to verify delivery.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used in accordance with stated practices in this PIA?

mLINQS is used internally to maintain and store pertinent employee and relocation expense data. It uses its features and flexible controls to automate and streamline the PCS travel cost management process, eliminating errors and simplifying the enforcement of complex federal policy throughout the Agency. mLINQS uses user entered information (PII) for the sole purpose of paying move related expenses of Federal Employees. A tracking system for transactions are in place to ensure unauthorized changes have not been made.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

To maintain their access, all users must attend all required as well as read and adhere to the Security Rules of Behavior for mLINQS Users. Annual user training on Information Security and privacy awareness

5.3 <u>Privacy Impact Analysis</u>: Related to Auditing and Accountability

<u>Privacy Risk</u>:

That audits are not completed, and the safeguards implemented are not followed.

<u>Mitigation</u>:

Administrative personnel are trained in the use of the tools in place to monitor and report suspicious activity, users are required to complete all required security awareness training annually and adhere to the Rules of Behavior for mLINQS users.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

mLINQS is used internally to maintain and store pertinent employee and relocation expense data. It uses its features and flexible controls to automate and streamline the PCS travel cost management process, eliminating errors and simplifying the enforcement of complex federal policy throughout the Agency.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ No___. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or*

other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.)

Last name or a relocation document control number assigned by the Business and Development Services Branch (BDSB) (Relocation Branch).

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

EPA-29 The SORN will be modified to incorporate the changes to the mLINQ's system as it moves to the Microsoft Azure Government Cloud as a Software as a Service (SaaS)

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

That the information is used for something other than completing relocation documentation.

Mitigation:

Multiple roles are used to enter/review the information to assure it is handled properly and a very small staff comprises the BDSB branch reducing the number of people who have access to this information.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Any individual who wants to know whether this system of records contain a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA FOIA Office, Attn: Privacy Act Officer, MC2822T, 1200 Pennsylvania Avenue, NW, Washington, DC 20460.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

mLINQ's does not share information with other agencies. We only ask for information necessary to process move requests and make payments on the users behalf therefore, users must provide requested information. Information is accessible only to Federal Government staff that are authorized to access the information to perform the required tasks. Opt out option is to not be reimburse. Risk of refusal to be reimbursed

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent. Welcome screen popup notification (warning banner)

Privacy Risk:

Minimal risk as access is on an as needed basis. Risk is users don't actually read the terms of service

Mitigation:

Any collected information is stored in secure servers in the Azure Cloud. Reminder screen when logging into mLINQS

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to their own personal information in this system of records will be required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required as warranted. Requests must meet the requirements of the EPA regulations at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Requests must be submitted to the Agency contact indicated on the initial document for which the related contested record was submitted.

8.3 How does the system notify individuals about the procedures for correcting their information?

Any individual who wants to know whether this system of records contain a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA FOIA Office, Attn: Privacy Officer, MC2822T, 1200 Pennsylvania Avenue NW., Washington, DC 20460.

8.4 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

None, there is appropriate procedure in place related to redress.

Mitigation:

None