

PRIVACY IMPACT ASSESSMENT

(Rev 2/2026 – All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.

All entries must be Times New Roman, 12pt, and start on the next line.

If you need further assistance, contact your LPO. A listing of the LPOs can be found here:

https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: mLINQS		System Owner: Adil Gulamali	
Preparer: Eric Kim		Office: OFA	
Date: 08/01/2026		Phone: 703-209-9144	
Reason for Submittal: Update to new template			
New: ☐	Revised: ☐	Annual Review: X	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: X	Rescindment/Decommission: ☐		
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 move LINQ 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.

Move LINQ Relocation Software, also known as mLINQS, is an EPA major information system (MIS). mLINQS has been operational since May 2006. In 2021 the mLINQS System transitioned to the mLINQS Hosting Service (MHS) a FedRAMP SaaS (Software as a Service) application hosted on the Microsoft Azure Cloud. The Environmental Protection Agency (EPA) uses mLINQS to help manage the Business Development & Services Branch (BDSB) Federal Employee Relocation Center (FERC),

which processes employee relocation moves for the EPA and several other external federal agencies. In 2025, mLINQS began winding down operations and no longer accepted new relocation requests. In addition, the EPA relocations were awarded to the Department of Veterans Affairs, which will process any new relocation requests. Exiting relocations already in process will be completed, and estimated system decommissioning is expected by late 2028 or early 2029.

Section 1. 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?

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. Privacy Act of 1974, as amended, 5 U.S.C. 552a, Pub. L. 93-579. OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, Appendix I. OMB Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" Privacy Act Implementation, Guidelines and Responsibilities, July 9, 1975.

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?

The current ATO expires April 30, 2028

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. 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). This information is no longer collected but stored for the existing

relocations.

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 by coming directly from the source. All information goes through a two-step process: one individual enters the data, and a second individual confirms it. This process is called a quality audit check. No new data is entered into the application, as it is not processing new relocation applications.

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:

As mLINQS is no longer processing relocations, there is minimal Privacy Risk. The only risk would be misuse of information by an administrator,

Mitigation:

Audit log review for any unusual activity.

Section 3. 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?

mLINQS does not have users other than the relocation staff. Only 5 staff members can access the application, and they need administrative rights to process existing relocations.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

There is no longer access to the system for users, since the application no longer accepts

relocation processing requests.

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

Only the relocation staff have access to the system, and they have privileged user roles.

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?

Only the relocation staff can access the information, and they are all EPA employees with approval to manage the application.

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 A number.

mLINQS records are retained for 10 years after file closure per EPA Records Schedule 1006B. OCFO reviews the record control schedules attached to their systems annually to ensure they are following the schedules for retiring and destroying the files. OCFO works with its records liaison officers to ensure the appropriate records control schedules are attached to the files. mLINQS disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with Records Schedule 1006B using secure methods.

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:

There is almost no privacy risk as only 5 administrators have access to the data and the number of records stored in the system is very low so even a breach would have little impact. The only risk would be insider threat if an administrator were to improperly misuse the data.

Mitigation:

As only administrators use the system the ISSO reviews activity weekly for unusual activities.

Section 4. 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?

It does not.

4.4 Does the agreement place limitations on re-dissemination?

It doesn't have limitations because it goes directly to the IRS

4.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There isn't a privacy impact as mLINQS staff submit data directly to tax agencies.

Section 5. 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 as stated in Section 6.1?

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) solely for the purpose of paying move-related expenses for Federal Employees. A transaction-tracking system is 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 complete all required training and read and adhere to the Security Rules of Behavior for mLINQS Users—annual user training on Information Security and Privacy awareness. As there are no longer any users with access to the system, there's no training necessary.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

There is no privacy risk as the system no longer has users. Audit logs can track all activity, and with only 5 administrative users with access to the system, activity is minimal and any activity is easily seen.

Mitigation:

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

mLINQS is used internally to maintain and store pertinent employees 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: ☒ 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 Office of Financial Operations – Cincinnati Finance Division).

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

SORN EPA-87 Records are stored but no longer disseminated. There is no risk to privacy unless it is an internal breach within the relocation department.

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:

The staff is trained to handle relocation and the information provided is only applicable to the relocation process. All activity can be audited and with only 5 remaining users it's very simple to log into activity from each account.

Mitigation:

Audit Log reviews for unusual activity.

If no SORN is required, STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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 contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

MlinqOffice does not share information with other agencies. We only ask for information necessary to process requests and make payments on the users' behalf; therefore, users must provide requested information. Information is accessible only to Federal Government staff authorized to access it to perform the required tasks. The opt-out option is to decline reimbursement. The risk of refusal would mean the individual would not 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.

Privacy Risk: No longer applicable as there are no new users of the system.

Mitigation: As relocations are no longer processed there are no notices so there is no mitigation.

Section 8. 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 information in this system of records about themselves are 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 EPA regulations implementing the Privacy Act of 1974 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. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.

8.3 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 Freedom of Information Act (FOIA).

Privacy Risk: N/A

Mitigation:

I attest as the Agency Privacy Officer that mLINQS Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA

**ROBERT
KELLY**

Digitally signed by
ROBERT KELLY
Date: 2026.09.28
10:20:04 -04'00'