Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Relocation (moveLINQ Application)

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 08/03/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
Office of Financial Management / Relocation

Unique Project Identifier: Relocation is an EAS OS-059 Application

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system

- Relocation is a child system of the EAS application system boundary.

(b) System location

- The system is primarily managed by resources located at the CBS Solutions Center in Gaithersburg, MD. The system is physically located at the Federal Aviation Administration Data Center (DOT/FAA/ESC) in Oklahoma City, OK.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

- There are no interconnections to external applications for the systems.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

- The moveLINQ application tracks all individual relocation expenses associated with moving an employee and their family members. It fully automates the requirements of the Federal Travel Regulations - chapter 302, the Department of State Standardized Regulations, and IRS Publications related to relocation payments. The application manages and tracks all aspects of government change of station and taxable Temporary Duty (TDY) travel allowances. Users from the NIST and NOAA travel groups manually enter information regarding relocation activities of employees and the system will calculate the appropriate per diem rates as well as tax information related to the move. This information stored is tied to a unique identification number (system generated) for each relocation.

(e) How information in the system is retrieved by the user

- Users access system information through a web based application.

(f) How information is transmitted to and from the system

- Information is transmitted over the DOC network to the user workstations.

(g) Any information sharing conducted by the system

- Information may be shared within the Department.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

- Budget and Accounting Act of 1921; Accounting and Auditing Act of 1950; and

Federal Claim Collection Act of 1966)

- Includes the following, with all revisions and amendments: 5 U.S.C. 301; 44

  U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; Executive Order 12564; Public Law 100-71, dated July 11, 1987

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

- Relocation is a child of EAS OS-059, which is categorized as MODERATE.

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017).

X___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	

e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: SSN is collected to generate the W-2 and other necessary tax information for the traveler to be completed for reimbursement.					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address	X	q. Military Service	
d. Gender		k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify): Employee's children's names and DoBs. Federal, state, and FICA taxes paid on behalf of the traveler being relocated (Relocation Income Tax Allowance (RITA)). Travel itineraries. Real estate sale, purchase, lease termination, and relocation service company amounts.					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address		i. Business Associates	
b. Job Title		f. Salary	X	j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax		Online	
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

All information is provided directly from the traveler. Travelers have the ability to review all documents specific to their reimbursement by sending a formal request to update their information through the Bureau Travel Group. Once requested, the documentation is sent to the individual via encrypted email.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): To provide Relocation Reimbursement Payments			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

The data contained in moveLINQ is being collected to support the travel relocation process and to ensure that the federal traveler incurs and receives the correct payments and reimbursements associated with their expenses.

The moveLINQ application has the functionality to create file exports to create required tax forms to provide to the IRS and employees for annual tax filing. This functionality is currently not used and it requires purchasing additional software. This PIA will be updated to reflect this process if the functionality is used in the future. Currently, instead of using moveLINQ tax form functionality, data is exported and bulk transferred into NIST and NOAA's tax form applications.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate

handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Paper documents are maintained until the information has been uploaded into the application. Once the documents are uploaded, the paper documents are immediately shredded. The data is maintained in the application for a period of two years then they are automatically deleted within application. Annual Cybersecurity Awareness Training is conducted in order to communicate the appropriate procedures for handling and dispensing of information. All users are required to sign the Rules of Behavior, which outline the data protection requirements, prior to being granted access to the application, annually, and whenever the rules have been updated.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X	X	
DOC bureaus	X	X	
Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

X	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

X	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: The moveLINQ production environment delivers data to the NIST and NOAA production instances of CBS by uploading bulk files to the SFTP server. NIST and NOAA then download the data from their respective SFTP servers and upload it into their respective CBS instances. The moveLINQ test environment connects to the NIST and NOAA test instances of CBS for the sole purpose of testing and development. This environment will remain for the entirety of the Relocation lifecycle. Only test data created for the sole purpose for testing will be housed in the test environment. No PII/BII is used for testing.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	X
Contractors	X		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. A Privacy Act statement is provided to all Travelers on each form they must complete. Forms used by Relocation are CD-150, CD-29, CD-369, CD-370 and Travel Vendor form (https://connection.commerce.gov/collection/commerce-department-forms)	
X	Yes, notice is provided by other means. A privacy notice is displayed to the users of the system before logging into Relocation application	Specify how: : "Warning - You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and for any lawful Government purpose, the

		Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicate your understanding of this warning. – Warning"
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: If an individual does not provide the required forms, they will not receive reimbursement for their relocation expenses.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: If an individual provides the required forms to the travel office, their data will be entered into the Relocation application and they will receive reimbursement for their relocation expenses.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Traveler can review all documents specific to their relocation reimbursement maintained in the moveLINQ application by requesting copies from the Bureau Travel Group. Inaccurate data will be corrected upon notification to the Bureau Travel Group.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 8/8/2020 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Access to the moveLINQ application is role based. Security is provided by granting and revoking privileges on a person-by-person and role-by-role basis. Temporary or emergency accounts are not allowed. In order to obtain access to the moveLINQ application the potential user must have their supervisor's (Group Leader, Division Chief or Administrative Officer) and the Travel Group's approval. The user must fill out a moveLINQ access request form and have their supervisor's (Group Leader, Division Chief or Administrative Officer) and the Travel Group sign the form. Users only have access to data that is required to perform their jobs. The moveLINQ application captures user ID information on transactions performed within the application. In addition, it maintains audit records for all transactions executed within the application. All sessions with the moveLINQ applications are encrypted from the user's computer to the application via TLS 1.2 encryption. All databases storing moveLINQ data are encrypted to protect the information at rest.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

X Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-1.html COMMERCE/DEPT-9 Travel Records (Domestic and Foreign) of Employees and Certain other Persons. http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-9.html COMMERCE/DEPT-18 Employees Personnel Files Not Covered By Notices of Other Agencies http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: GRS 1.1 Financial Management and Reporting Records http://www.archives.gov/records-mgmt/grs/grs09.pdf
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

	Identifiability	Provide explanation:
X	Quantity of PII	Provide explanation: The moveLINQ data will maintain personal information on all Department of Commerce employees and their spouse, dependents, or otherwise involved in relocation reimbursement.

X	Data Field Sensitivity	Provide explanation: The PII contained in moveLINQ, could be used maliciously against users resulting in loss of funds, identify theft , etc.
X	Context of Use	Provide explanation: Provide explanation: Information is collected for administrative purposes to re-reimburse travelers and relocation expenses.
X	Obligation to Protect Confidentiality	Provide explanation: Promises of confidentiality regarding the information have been conveyed to the subject individual at the time or point of collection, and information is afforded confidentiality from unauthorized disclosure by statute or regulation (Privacy Act of 1974).
X	Access to and Location of PII	Provide explanation: Access is to the moveLINQ application only and granted on a person-by-person and role-by-role basis. Access is limited to necessary Travel Group personnel and the potential user must have their supervisor's (Group Leader, Division Chief or Administrative Officer) and the Travel Group's approval before obtaining access to the moveLINQ application. The servers are located at the Federal Aviation Administration (FAA) Enterprise Service Center in Oklahoma City, Oklahoma. There is a Service Level Agreement (SLA) with the FAA to host the application servers.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

After a review of the threats associated with the application, it was determined that since this application is primarily used for administrative support, a potential risk of insider threat was noted. To protect against this, each user is provided with annual cyber security training outline how to maintain and access systems with PII. Also, role-based protections are in place to ensure that users can access data that is only allocated to their bureau/role/level. Audit logs are captured in the system and retained for after the fact investigations. Audit Logs are reviewed in support of event investigations on an as needed basis.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.