U.S. Department of Commerce
Office of Financial Management

Privacy Threshold Analysis
for the
Relocation Application

U.S. Department of Commerce Privacy Threshold Analysis

Office of Financial Management / Relocation

Unique Project Identifier: Relocation

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) *Whether it is a general support system, major application, or other type of system*
   - Relocation is a Minor System, and a child system of the EAS application system boundary.

b) *System location*
   - Physically located at the DOTESC Data Center in Oklahoma City, OK.
   - Relocation Management Office is located at the CBS Solutions Center in Gaithersburg, Maryland.

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.

d) *The purpose that the system is designed to serve*
   - The Relocation application is the moveLINQ application from mLINQs. This licensed application manages the authorization and invoicing for Department of Commerce employee relocation.

e) *The way the system operates to achieve the purpose*
   - Relocation manages its authorization and invoicing through an interface with CBS and the tax documentation for employee relocation.

f) *A general description of the type of information collected, maintained, use, or disseminated by the system*
   - Relocation collects supporting documentation from the person being relocated such as Driver's License number, Vehicle ID, Credit Card information.

g) *Identify individuals who have access to information on the system*

- Relocation is accessed by authorized moveLINQ users authorized based on their job function.

h) *How information in the system is retrieved by the user*

- Users access system information through a web based application.

i) *How information is transmitted to and from the system*

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

Questionnaire:

1. What is the status of this information system?

_____ This is a new information system. *Continue to answer questions and complete certification.*

_____ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

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. *Continue to answer questions and complete certification.*

__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 01-2015 or later). *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

   NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

_____ Yes. *Please describe the activities which may raise privacy concerns.*

_____ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

   As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

_____ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

_____ Companies
_____ Other business entities

_____ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

_____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

_____ DOC employees
_____ Contractors working on behalf of DOC
_____ Members of the public

_____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

_____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

_____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.
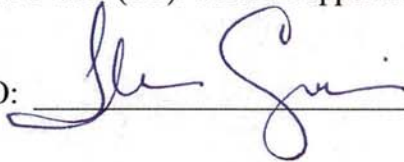
CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Relocation and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the Relocation and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Teresa Coppolino

Signature of SO: _____ Date: 4/19/18

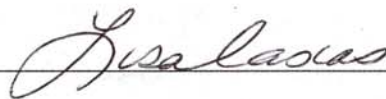Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO: _____ Date: 4/23/2018

Name of Authorizing Official (AO): Lisa Casias

Signature of AO: _____ Date: 4/30/18

Name of Bureau Chief Privacy Officer (BCPO): Kathleen Gioffre

KATHLEEN GIOFFRE
Digitally signed by KATHLEEN GIOFFRE
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=KATHLEEN GIOFFRE, 0.9.2342.19200300.100.1.1=13001000075444
Date: 2018.04.24 08:26:05 -04'00'

Signature of BCPO: _____ Date: _____