

**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: An EAS OS-059 Application

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 on 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: *Provide a brief description of the information system.*

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).

The Relocation application is the moveLINQ software from mLINQS. This licensed application manages the authorization and invoicing for Department of Commerce employee relocation through an interface with CBS, as well as the tax documentation for employee relocation. At this time, this application is hosting NIST and NOAA relocation activities. The moveLINQ application is housed at DOTESC and interfaces with the NIST and NOAA CBS applications, housed at NIST and NOAA; by transferring XML files through the DOTESC SFTP. Only the NIST and NOAA travel groups, NIST and NOAA moveLINQ administrators, and some OFMS system administrators have access to the production application.

Address the following elements:

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, MD.

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, used, or disseminated by the system

Relocation collects supporting documentation from the person being relocated such as Driver's License Number, Vehicle ID, and 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. Status of the Information System****1a. 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. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

- _____ Yes. This is a new information system.
- _____ Yes. This is an existing information system for which an amended contract is needed.
- _____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.
- _____ No. This is not a new information system.

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. *(Check all that apply.)*

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

_____ 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.

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

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

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

- _____ DOC employees
- _____ Contractors working on behalf of DOC
- _____ Other Federal Government personnel
- _____ 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 Social Security numbers (SSNs), including truncated form?

_____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
--

Provide the legal authority which permits the collection of SSNs, including truncated form.

_____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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, 4c, and/or 4d are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PIA and the SAOP approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION

 X The criteria implied by one or more of the questions above **apply** to Relocation and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

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

<p>Information Technology Security Officer Name: Eduardo Macalanda Office: DOC OFMS Phone: 301-355-5987 Email: emacalanda@doc.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>	<p>Chief Information Security Officer Name: Densmore Bartley Office: OS OCIO Phone: 202-482-3186 Email: dbartley@doc.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>
<p>System Owner Name: Teresa Coppolino Office: DOC OFMS Phone: 301-355-5501 Email: tcoppolino@doc.gov</p> <p>I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.</p> <p>Signature: _____</p> <p>Date signed: _____</p>	<p>Authorizing Official Name: Dr. Lawrence W. Anderson Office: OS OCIO Phone: 202-482-2626 Email: landerson@doc.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>
<p>Authorizing Official Name: Stephen M. Kunze Office: Office of Financial Management Phone: 202-482-3709 Email: skunze@doc.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>	<p>Privacy Act Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>

<p><i>Section intentionally left blank.</i></p>	<p>Bureau Chief Privacy Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202-482-8075 Email: tmurphy2@doc.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: _____</p> <p>Date signed: _____</p>
---	---