## 1. Contact Information

**Department of State Privacy Coordinator**
Margaret P. Grafeld
Office of Information Programs and Services
Information Sharing Services
Bureau of Administration

## 2. System Information

(a) Date PIA was completed: 5/15/2008

(b) Name of system: Language Services Job Tracker

(c) System acronym: LSJT

(d) IT Asset Baseline (ITAB) number: XXX

(e) System description (Briefly describe scope, purpose, and major functions):

This system is used to schedule and track Interpreting/translation jobs performed by staff members as well as contractors. It does keep track of the contractors used by Language Services.

(f) Reason for performing PIA:

☐ New system

☒ Significant modification to an existing system

☐ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): This is an annual update to the privacy impact assessment for LSJT. A/EX/IRM previously provided a PIA during the certification and accreditation of the application in November 2007.

(h) Date of previous PIA (if applicable): November 2007

## 3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

### a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The PII collected is: Social Security Numbers, dates of birth, name, address, Data Universal Numbering System (DUNS), telephone numbers (home and work), e-mail addresses, and financial account numbers. The source of the information is provided by the Individual on a paper application.

### b. How is the information collected?

The individual completes an application form manually. A/OPR/LS then inputs the data from the hard copy form into the LSJT database.

### c. Why is the information collected and maintained?

Collection of the PII is necessary to create a user profile in Travel Manager. Travel Manager then provides this information to GFMS for completion of the travel forms and travel vouchers.

### d. How will the information be checked for accuracy?

The applicant manually checks his/her information prior to submission to the A/OPR/LS staff. The A/OPR/LS staff then ensures the information entered into LSJT matches the information on the applicant's form. The LSJT application then has automated data integrity checks, ensuring information entered into certain data fields matches the requirements for the field to actually accept and process the data. Furthermore, LSJT sends an automated mass email to all applicants annually asking applicants to verify any changes to their information. (Note: no PII is distributed with this mass mailing.)

### e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

22 U.S.C. 811A.

### f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

LSJT collects only the minimal amount of PII required for the A/OPR/LS staff to contact applicants and to process travel requests and reimbursements. LSJT does not allow for the creation of additional fields, prohibiting end users from collecting more data than is initially required. Furthermore, role-based access controls are in place on the database. Only database administrators have the capability to alter the database. Their privileges are reviewed annually under the principle of least privilege. Additionally, LSJT users possess only those rights/permissions that allow them to do their job within the database.

## 4. Uses of the Information

### a. Describe all uses of the information.

All PII (except for the DUNS) is supplied to the Travel Manager system to establish the users' profiles, which are eventually used to create travel forms and travel vouchers. The DUNS is submitted to GFMS for processing an applicant's financial claims.

### b. What types of methods are used to analyze the data? What new information may be produced?

When the data is entered into LSJT, the data is stored until required. LSJT users run reports to analyze potential applicants for certain jobs and to process other applicants requiring travel submissions. The information is transferred to Travel Manager which provides the data to GFMS but not to any other entity.

### c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

No, this system does not use any of this information.

### d. Is the system a contractor used and owned system?

No, the system is developed, maintained, and owned entirely by Department of State.

### e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

The Office of Information Assurance checked and verified over 257 security controls during the certification and accreditation process in November 2007. All roles and responsibilities detailing role based access to the data are highlighted in the System Security Plan (SSP).

## 5. Retention

### a. How long is information retained?

The information is retained in accordance with the disposition schedule which is from 5-6 years. The data is then retired according to the retention schedules of DoS published schedules.

### b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

The PII is stored on a certified and accreditated information system. Back up media housing the PII for DoS is then stored in secondary alternate facilities in secure, access controlled rooms with Unicam cipher locks. The information is utilized by A/OPR/LS and is transferred to Travel Manager through FIPS140-2 network encryption. The security controls in place for Travel Manager have also been certified and accredited as well.

## 6. Internal Sharing and Disclosure

### a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The information is utilized by Internal users and is transferred to Travel Manager by manually entering information in the Travel Manager Web portal. It is then transmitted via FIPS140-2 network encryption. The security controls in place for Travel Manager have also been certified and accredited. NOTE: the LSJT does not have any interdependencies with any other information system. A/OPR/LS staff retrieves information from the LSJT database and then manually enters the information into the Travel Manager system.

### b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

The LSJT database does not support any automated means to share information. When information is extracted from LSJT and used in Travel Manager, the information is

entered into the Travel Manager Web portal and is transmitted via FIPS140-2 network encryption.

**c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.**

Not applicable since there is no internal sharing of data.

## 7. External Sharing and Disclosure

**a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?**

No data is shared with external organizations.

**b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?**

Not applicable because data is not shared with external organizations.

**c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.**

Not applicable because data is not shared with external organizations.

## 8. Notice

The system:

X constitutes a system of records covered by the Privacy Act.

☐ Does not constitute a system of records covered by the Privacy Act.

**a. Is notice provided to the individual prior to collection of their information?**

A notice was published in the Federal Register prior to collection of the public's information. The System of Record Notice covering this collection is entitled Translators and Interpreters Record, STATE-37.

**b. Do individuals have the opportunity and/or right to decline to provide information?**

Yes, the individual has the choice to not submit an application. Internal users can decline to provide information, exit the application, and a record will not be created. No penalties or denial of a right, benefit, or privilege will result from this action

**c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?**

No. All information is required to process an individual's application.

**d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.**

The System of Records Notice Translators and Interpreter Record STATE-37 was published in the Federal Register for the public comment period of 40 days prior to collection. The notice is available on the Department of State public facing website and the Federal Register for review. The notice provide individuals with the type of information the system collects, the routine use of the information, and notification procedures. This information is also provided prior to collection.

## 9. Notification and Redress

**a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?**

The records of the individuals whose information was collected have notification and redress rights under the Act, and the relevant procedures are or will be described in CFR rulemaking and the SORN. Individuals who want to gain access or to amend their records should write to the U.S. Department of State, Attn: Director, Office of Information Programs and Services, Washington DC 20522-8001.

**b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.**

The notification and redress procedures offered to individuals are reasonable and adequate in relation to the system's purposes and uses. This information was published 40 day prior to collection and the procedures are available on the Department of State public-facing website. There may be instances in which individuals are not aware of the existence of the procedures; however, the Department has made every attempt prior to collection to inform individuals of the procedures to prevent any privacy risks.

## 10. Controls on Access

**a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?**

Only DoS-badged individuals who are pre-approved and authorized by the Director and his/her deputy are granted access to the database. To provide database administrative support requires that database administrators have full access. Internal users have limited, restricted user rights to access the information on an "as needed basis" to process the applicant's information and/or Travel Manager. The database and server have mandatory auditing to identify any unauthorized access or modifications to the data. These were all verified during the certification and accreditation of the application during November 2007.

**b. What privacy orientation or training for the system is provided authorized users?**

Roles and responsibilities as well as Rules of Conduct have been established and training has been conducted regarding the handling of PII. The initial training consists of computer security awareness to include the handling of PII. The mandatory refresher training covers security awareness which also includes the handling of PII. Furthermore, there is an annual security brief which includes the handling of PII. Information has been provided under the Privacy Act of 1974. Users are verbally briefed on the sensitivity of PII data before they use the system for the first time.

### c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

The residual risk is detailed and compensated in the Plan of Action and Milestones (POAM) as annotated in the CIO's authorization of the application in November 2007.

## 11. Technologies

### a. What technologies are used in the system that involves privacy risk?

All technologies used in the system have compensating controls for associated privacy risks and are also equipped with sufficient antivirus software.

### b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

All technologies used were certified and accreditated by the Office of Information Assurance during November 2007. The technologies may cause risk if they're not patched or utilize sufficient antivirus software. All servers associated with it have compensating controls for associated risks as identified in Diplomatic Security's Security Configuration Guidelines.

## 12. Security

### What is the security certification and accreditation (C&A) status of the system?

The system was been certified and accredited in November 2007 for three years.