



Privacy Impact Assessment
for the

Relocation Tracking System (RTS)

February 28, 2007

Contact Point
Office of Information Systems
Drug Enforcement Administration
(202) 307-1000

Reviewing Official
Jane C. Horvath
Chief Privacy Officer and Civil Liberties Officer
Department of Justice
(202) 514-0049

Introduction

The Relocation Tracking System (RTS) is used by the Office of Acquisition Management to administer the relocation of agency employees.

Section 1.0 The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The Relocation Tracking System (RTS) collects the following employee information:

- full name,
- Social Security Number (SSN),
- home address,
- pay grade,
- job series,
- full name of spouse,
- inventory of household goods,
- names and birth dates of dependents involved in a relocation of an employee, and
- the employee's Vehicle Identification Numbers (VINs) of privately owned vehicles (POVs).

1.2 From whom is the information collected?

RTS information is collected from transferring / relocating agency employees.

Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

The information in RTS is used to determine and calculate estimated expenses to be incurred by the agency by relocating the employee. The SSN is collected in order to be printed on authorizing documents that accompany employee vouchers.

Section 3.0

Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The information is used to administer employee relocations and associated actions. It is used by the RTS system to produce authorization documents (travel orders and authorizations for the transportation & storage of goods), and track invoices from companies providing relocation services. These services are the transportation & storage of goods and the sale of residences. The software also uses the information to produce form letters sent to employees and to General Services Officers (GSOs) at American embassies in countries to/from which employees are moving. RTS is sometimes used to facilitate retrieval of information from the agency's financial system.

The agency creates an internal control number called a "TCN" for each relocation of an employee. This TCN is stored along with other information related to each action processed by the software.

The information is also used to compile statistics used to make policy decisions and to respond to requests for statistics from other offices and agencies.

Section 4.0 Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

The personally identifiable information is not shared outside of the component.

Section 5.0

External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

An employee's name is provided to the GSO at the American Embassy in the foreign country to and/or from which the employee is moving.

An employee's name, telephone number, home address and TCN are provided to goods carriers (moving companies). When the company is shipping a POV, the VIN is also provided.

Companies storing an employee's goods receive the employee's name, post of assignment and TCN.

Relocation companies receive an employee's name, telephone number, home address and TCN. Occasionally, the name of the employee's spouse is provided to relocation companies.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes. However, travel orders will not be issued and therefore their relocation expenses will not be paid by the government.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Yes. Providing the information implies consent to use it to facilitate the relocation at government expense. The individual can decline consent by not providing the information.

Section 8.0

Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Threat: Unauthorized Access to RTS

Risk: Low

Mitigation / Countermeasures:

- Authentication controls. Initial access to RTS is limited to authorized users with active RTS accounts on a closed Sensitive But Unclassified (SBU) local area network (LAN) called Firebird. Multi-layered security is in effect by virtue of the fact that users must first logon to Firebird and then access RTS after a successful Firebird authentication. An unauthorized user would have to have knowledge of both userID/password combinations in order to gain access to RTS.
- Role-based access controls. Access to specific data is restricted by user classification. Additionally, the detail level of the information available is limited by the user classification.
- Access and changes to RTS data can be tracked through database logging and auditing. Auditing logs are checked on a routine basis and monitored by system administrators.
- RTS user accounts can be created, updated, enabled and disabled only by authorized administrators. In order to perform these functions, individuals must be identified as a System Administrator.
- RTS is hosted within the DEA's Firebird SBU LAN and Firebird is fully Certified and Accredited (C&A) according to generally accepted guidelines for C&A of systems for DOJ and re-accredited every 3 years. In addition, the system is also scrutinized annually with system self-assessments that verify and validate that the appropriate security measures are being effectively deployed.

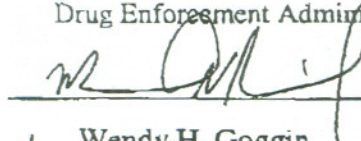
Conclusion

RTS is used by DEA's Office of Acquisition Management to administer the relocation of agency employees. Information is collected from employees to estimate relocation costs and to produce authorization documents. RTS resides on the Agency's SBU LAN, which provides multi-layered information security.

Responsible Officials

 <<Signature>> 3-23-2007 <<Date>>

for James D. Craig
Assistant Administrator ACTING
Chief Privacy Officer
Drug Enforcement Administration

 <<Signature>> 3/21/07 <<Date>>

for Wendy H. Goggin
Chief Counsel
Chief Privacy Official
Drug Enforcement Administration

Approval Signature Page

 <<Signature>> 4/5/07 <<Date>>

Jane Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice