Name of Project: International Treasury Services (ITS.gov)
Department: Department of Treasury
Bureau: Financial Management Service
Project's Unique ID: ITS.gov

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes

a. Is this information identifiable to the individual[1]?

Yes.

Is the information about individual members of the public?

Yes.

Is the information about employees?

Yes.

What is the purpose of the system/application?

ITS.gov is a web-based international payment system that enables Federal government agencies to make payments in foreign currencies via direct deposit, wire transfer, or foreign draft to recipients overseas.

What legal authority authorizes the purchase or development of this system/application?

31 U.S.C. § 3332

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Any individual located overseas that is a recipient of a Federal government payment may be covered in the system.

2) What are the sources of the information in the system?

The Federal agency provides the information either to an FMS Regional Financial Center or directly to ITS.gov

Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

ITS.gov receives the information either from other Federal agencies or from FMS Regional Financial Centers (which receive the information from other Federal agencies). The ultimate source of the information is the individual, who provides the information to the Federal agency issuing the payment.

a. What Federal agencies are providing data for use in the system?

ITS.gov receives payment files from FMS Regional Financial Centers and Federal government agencies.

What Tribal, State and local agencies are providing data for use in the system?

N/A, information is not obtained from Tribal, State or local agencies.

b. From what other third party sources will data be collected?

N/A, information is not obtained from third party sources.

c. What information will be collected from the employee and the public?

The individual's name, Social Security Number, employee identification number, home address (or business address for vendors), and bank account number may be collected from the public.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than FMS records be verified for accuracy?

It is the responsibility of the Federal agency to provide accurate data in order to process payments using ITS.gov.

b. How will data be checked for completeness?

It is the responsibility of the Federal agency to provide accurate data in order to process payments using ITS.gov.

Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

It is the responsibility of the Federal agency to provide current data in order to process payments using ITS.gov.

Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, data elements and a brief description are maintained in the Business Information Services Design Document (dated September 15,2004).

C. ATTRIBUTES OF THE DATA:

1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

The system does not derive or create new data.

3) **Will the new data be placed in the individual's record?**

N/A

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

N/A

5) **How will the new data be verified for relevance and accuracy?**

N/A. New data is not being derived nor created by ITS.gov.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

ITS.gov software is in a controlled production system and there is no general-purpose user access. All user access is strictly controlled by the application.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

ITS.gov software is in a controlled production system and there is no general-purpose user access. All user access is strictly controlled by the application.

8) **How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Currently FRB personnel and authorized Federal agency personnel can retrieve data using personal identifiers including SSN, employee identification number, home address (or business address for vendors), and bank account number.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

ITS.gov administrators view the audit logs available in weekly on reports. The ITS.gov mainframe has similar audit features in the ITS.gov application. Unauthorized activities are reported and made available to system administrators who request them. These various audit reports are retrieved on a weekly basis to determine which Users are not using the system or have had invalid attempts at entering the system.

FRB personnel and authorized Federal agency users may also run a query on payment history. The query may provide payment detail which includes personal identifiers such as SSN, home address and bank account number.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

Although providing the requested information is voluntary, an individual's failure to provide information may delay or prevent Treasury from making a federal payment by direct deposit to the individual.

D. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The ITS.gov web front-end application resides in the Treasury Web Application Infrastructure (TWAI) and the mainframe resides in Federal Reserve facilities. There is an interface between the ITS.gov web front-end and the mainframe back-end to ensure consistent data.

Both the web front-end and the mainframe have contingency sites. Data is replicated between the primary site and the contingency site.

2) What are the retention periods of data in this system?

Records for payments are retained indefinitely unless explicitly approved for disposition. Records are retained in accordance with statute, court order or Treasury Directive 25-02, Records Disposition Management Program. Audit logs of transactions are retained for a period of six (6) months or as otherwise required by statute or court order

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Paper copies of reports are destroyed when no longer needed using approved destruction procedures for sensitive information. Data files to archive are retained indefinitely. Detailed procedures are contained in the ITS.gov Security Plan

4) Is the system using technologies in ways that the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No, ITS.gov technologies are consistent with ways FMS has previously employed payment technologies.

5) How does the use of this technology affect public/employee privacy?

N/A

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

ITS.gov administrators view the audit logs available weekly on the audit reports. The ITS.gov mainframe has similar audit features in the ITS.gov application. Unauthorized activities are reported and made available to Users who request them. These various audit reports are retrieved on a weekly basis to determine which users are not using the system or have had invalid attempts at entering the system.

FRB personnel and authorized Federal agency users may also run a query on payment history. The query may provide payment detail which includes personal identifiers such as SSN, home address and bank account number.

7) What kinds of information are collected as a function of the monitoring of individuals?

The ITS.gov application software provides auditing features that record user behavior within the application and within the host operating system

What controls will be used to prevent unauthorized monitoring?

ITS.gov software is in a controlled production system and there is no general-purpose user access. All user access is strictly controlled by the application.

8) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

Treasury/FMS .002 and Treasury/FMS .016

9) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

SOR Notices will not require amendment or revision.

E. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

The ITS.gov Program Office maintains a listing of all Federal Reserve, FMS, users at DoD, users at Federal agencies and contractor personnel authorized for ITS.gov access.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

ITS.gov defines access control policy, groups and individual user permissions based on least privilege. Access and permissions are restricted to the approved domain. Granting of initial or change in access or permissions must be accomplished in writing and approved by an authorized Head of Organization.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

User access will be restricted. Federal agency users will be restricted to accessing only their Federal agency data. Users with administrative privileges are restricted to the minimum necessary.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

ITS.gov application contains an access control module. Users are defined in an LDAP user directory. Roles have been defined and are used to grant access to each individual commensurate with the user's need.

Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes.

Do other systems share data or have access to the data in the system? If yes, explain.

Other systems provide data to ITS.gov, because ITS.gov receives payment files from FMS Regional Financial Center systems and other Federal government agencies. However, other systems do not have access to data in ITS.gov.

5) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The information owner and system manager share responsibilities for protecting the privacy rights.

6) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

Federal government agencies will provide data to ITS.gov when they send payment files to ITS.gov and will have access to the data that they provide.

7) **How will the data be used by the other agency?**

Federal agencies will have access to data in the system for reporting and/or auditing purposes.

8) **Who is responsible for assuring proper use of the data?**

The ITS.gov Program Office.