Financial Management Service

Privacy Impact Assessment

The Financial Management Service (FMS) Mission is to provide central payment services to Federal Program Agencies, operate the federal government's collections and deposit systems, provide government-wide accounting and reporting services, and manage the collection of delinquent debt owed to the government.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html

Document Date: June 9, 2011

Document Version: 1.0

Name of System: ITS.gov

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

ITS.gov is the Federal Government's enterprise-wide solution for international payments and collections. ITS.gov also performs OFAC screening services.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

ITS.gov operates under SORN Treasury/FMS .002 and Treasury/FMS .016.

3) If the system is being modified, will the SORN require amendment or revision?
__yes, explain

_X_no

4) Does this system contain any personal information about individuals?
_X_yes
__no

a. Is the information about members of the public?
Yes

b. Is the information about employees or contractors?
No

5) What legal authority authorizes the purchase or development of this system?

31 U.S.C. § 3332

DATA in the SYSTEM:

1) Identify the category of individuals in the system

Check all that apply:

__ Employees
__ Contractors
_X_ Taxpayers
__ Others (describe) (vendors that perform services on behalf of the Federal Government. Many vendors are located outside the United States)

2) Identify the sources of information in the system
Check all that apply:

__ Employee
__ Public
_X_ Federal agencies
__ State and local agencies
__ Third party

a. What information will be collected from employees or contractors?
None

b. What information will be collected from the public?
Beneficiaries who wish to receive their benefits via electronic deposit on a monthly basis must provide their Social Security Numbers, dates of birth, address and banking information.

c. What Federal agencies are providing data for use in the system?
Federal Program Agencies, Federal Benefit Units and the Treasury Department's Regional Financial Centers provide information for use in the ITS.gov application.

d. What State and local agencies are providing data for use in the system?
None

e. From what other third party sources will data be collected?
None

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources, other than FMS records, be verified for accuracy?
Federal Program Agencies and Federal Benefits Units have responsibility for providing accurate data to ITS.gov.

b. How will data be checked for completeness?
ITS.gov databases have required fields for beneficiary information.

c. What steps or procedures are taken to ensure the data is current?
Beneficiaries have responsibility for notifying Federal Benefits Units whenever addresses and/or banking information change. Federal Benefits Units have responsibility for notifying ITS staff whenever a beneficiary dies.

d. In what document(s) are the data elements described in detail?

The ITS.gov Data Dictionary contains a detailed inventory of application data elements.

ATTRIBUTES OF THE DATA:

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

   Beneficiary names, Social Security Numbers and addresses are unique identifiers to confirm the beneficiaries that are due beneficiary payments. ITS staff also uses this information to conduct OFAC screening due diligence. Banking information is necessary to settle payments

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

   No

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

   N/A

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

   No

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

   N/A

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

   ITS.gov access is limited to Federal government employees (and contractors) and Federal Reserve System staff.

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

   ITS.gov access is limited to Federal government employees (and contractors) and Federal Reserve System staff.

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

   ITS.gov users are assigned to an agency. Users only have access to information associated with their agency. Personal identifiers to retrieve information include name, Social Security Number, address, date of birth and banking information.

The ITS staff located at FRB New York and FRB Richmond have access to information on all agencies.

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

ITS.gov users are assigned to an agency. Users only have access to information associated with their agency. Users can generate reports to track the status of payments to beneficiaries and vendors.

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)? How can individuals grant consent?

Beneficiaries who wish to receive their benefits via electronic deposit on a monthly basis must provide their Social Security Numbers, dates of birth, address and banking information. Vendors must provide names, addresses and banking information. Upon request, vendors must also provide dates of birth, places of birth and/or purpose of payment as part of the OFAC screening due diligence process.

Failure to provide information could result in delayed payments and/or non-payment.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) What are the retention periods of data in this system? How long will the reports produced be kept?

ITS.gov maintains payment records for a period of seven years.

2) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?

The ITS CBAF staff at the Federal Reserve Bank of New York has responsibility for submitting an action request ticket to the Treasury Web Application Infrastructure (TWAI) environment for disposition of obsolete payment data.

The Treasury Department's record retention center in Lees Summit, Missouri has responsibility for destroying paper copies of ITS records after seven years.

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

ITS.gov is a web-based application that resides in the TWAI environment at FRB New York. ITS.gov has approximately 1,000 active users with the ability to access ITS.gov from anywhere in the world. Access control for most users is based on two-factor authentication using tokens. Access control for other users is based on user ID and password.

The TWAI environment has responsibility for ensuring the confidentiality, integrity and availability of the data.

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

No

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

N/A

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

No

7) What kind of information is collected as a function of the monitoring of individuals?

N/A

8) What controls will be used to prevent unauthorized monitoring?

N/A

ACCESS TO DATA:

1) Who will have access to the data in the system?
Check all that apply:

__ Contractors
_X_ Users
__ Managers
_X_ System Administrators
__ System Developers
__ Others (explain)_________

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

The ITS.gov Program Manager has responsibility for designating a Head of Organization (HOO) for each Federal Program Agency. The HOO has responsibility for designating an Authorizing Official (AO) who can request user access to ITS.gov. Access privileges are role-based and users only have access to the information associated with their agency.

ITS security administrators have responsibility for granting user access and assigning role-based privileges. All users must sign and acknowledge the ITS.gov Rules of Behavior before receiving access to the application.

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

ITS.gov is a role-based application. Users only have access to the information associated with their agency.

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 has strict access control policies to prevent the misuse of data. ITS.gov is a role-based application that follows the policies of least privilege and separation of duties. ITS.gov requires multiple users to complete tasks. ITS.gov also maintains audit logs that record user activity within the application. In addition, the Federal Reserve System's National Incident Response Team (NIRT) has responsibility for monitoring the TWAI environments for intrusion detection and incident response.

5) If contractors are/will be involved with the design, development or maintenance of the system were Privacy Act contract clauses inserted in their contracts and were other regulatory measures addressed?

Yes, The Federal Reserve Bank of New York, in its role as fiscal agent for the Treasury Department, has responsibility for the design, development and maintenance of the ITS.gov application.

6) Do other systems share data or have access to the data in the system?

__X yes
__no

If yes,

a. Explain the interface.

ITS.gov shares payment information with vendors and service providers. ITS.gov has interfaces with Citi and FedACH/FedGlobal via Connect:Direct. ITS.gov has an interface with LexisNexis via WebServices and a pending interface with FedWire via Message Queue.

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

The Federal Reserve Bank of New York, in its role as fiscal agent for the Treasury Department, has responsibility for ensuring vendors and service providers protect the privacy rights of the public and vendors affected by the interfaces.

7) Will other agencies share data or have access to the data in this system?

_X_yes
__no

If yes,

a. Check all that apply:
_X_Federal
__State
__ Local
__Other (explain) ________________

b. Explain how the data will be used by the other agencies.

Federal Program Agencies, Federal Benefit Units and the Treasury Department's Regional Financial Centers provide information for use in the ITS.gov application.

c. Identify the role responsible for assuring proper use of the data.

Each agency has responsibility for providing accurate information to ITS.gov. The Federal Reserve Bank of New York, in its role as fiscal agent for the Treasury Department, has responsibility for assuring proper use of the data once ITS.gov receives the data.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html