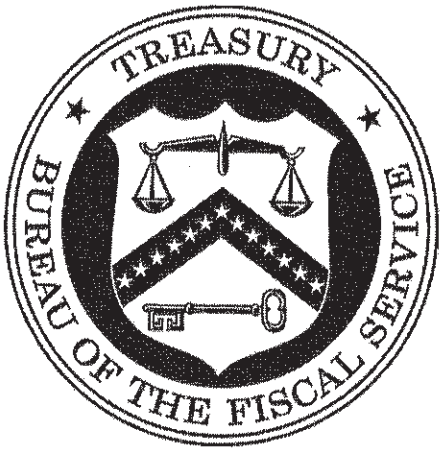

The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):
http://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: ITS.gov

Document Version: Version 3.0

Document Date: 4/26/16

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 process Treasury domestic wire payments and domestic accounts payments in the International ACH Transaction (IAT) format. ITS.gov screens all payments and collections for Office of Foreign Assets Control (OFAC) Compliance.

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

ITS.gov operates under SORN FMS .002 – Payment Records

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? Yes

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:
_x_ Employees
_x_ Contractors
_x_ Taxpayers
_x_ Others (describe)

Other individual categories include:
Vendors that perform services on behalf of the Federal Government. Many vendors are located outside the U.S.

Beneficiary categories include:
(1) Beneficiaries of Title II of the Social Security Act.
(2) Beneficiaries of Title XVI of the Social Security Act.
(3) Beneficiaries of the Civil Service Retirement System.
(4) Beneficiaries of the Railroad Retirement System.
(5) Beneficiaries of the Department of Veterans Affairs.

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?** None

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 Fiscal Service 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 and edits checks 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 (FBU) 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?**

Unique identifiers are used to confirm the beneficiaries that are due beneficiary payments. ITS staff also use this information to conduct OFAC screening due diligence. Banking information is necessary to settle payments. Data is necessary to ensure ITS remits payments to the appropriate recipients.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?** No

How will this be maintained and filed? N/A

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?** N/A

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

ITS contains various levels of checks and balances within the system for data verification and approval.

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. ITS staff designed the application to adhere to the policy of least privilege and prevent malicious activity without collusion. ITS.gov also adheres to the policy of separation of duties among users to prevent any one person from performing all functions of a business process.

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. ITS staff designed the application to adhere to the policy of least privilege and prevent malicious activity without collusion. ITS.gov also adheres to the policy of separation of duties among users to prevent any one person from performing all functions of a business process.

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. All ITS.gov user roles were designed in accordance with the policies of separation of duties and least privilege.

The ITS support staff has access to all agency information.

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 can generate reports that contain beneficiary name, address and banking information. Access is limited to the FBU staff, Office of International Operations (OIO) and the ITS Operation staff.

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.

ITS staff has access to information for all agencies

10) **What opportunities do individuals have to decline to provide information (i.e., in such cases 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 minimum 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?**

ITS staff have responsibility for submitting a disposition request to Payment Management for disposition of obsolete payment data. Payment Management's Records Management Liaison Officers (RMLO)
should be contacted to start the disposition process. The disposition of this system data is still subject to approval from Treasury's Office of Chief Counsel's approval. The Treasury Department has responsibility for destroying paper copies of ITS records that are stored at the Federal Records Center. The Federal Records Center notifies the Records Management Branch when records have reached their retention period and are scheduled to be destroyed.

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 relies on the infrastructure staff to conduct backups of user-level information contained in the information system. Intervals for data backup are daily for incremental data backups and weekly for full data backups.

ITS staff have responsibility for ensuring data backups exist for the ITS.gov documents stored in the shared network.

The ITS.gov application has a primary production and contingency production

location. ITS conducts annual failover tests.

4) **Is the system using technologies in ways that Fiscal Service has not previously employed**
(e.g., monitoring software, Smart Cards, Caller-ID)?
No, Fiscal Service has approved all ITS.gov technologies and the way ITS.gov is using the technologies.

5) **How does the use of this technology affect employee or public privacy?**
ITS.gov shares personally identifiable information (PII) with service providers. ITS has contractual agreements with all vendors to protect and safeguard all PII.

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

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
_x_ 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. HOOs and AOs can only request user access to information associated with their agency. HOOs and AOs also request a particular role for each user. ITS.gov developed each role in accordance with the policy of separation of duties and least privilege. ITS security administrators have responsibility for granting user access and assigning role-based privileges. Access privileges are role-based and users only have access to the information associated with their agency.

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. It is a rolebased
application that follows the policies of least privilege and separation of duties. ITS.gov requires multiple users to complete tasks. ITS.gov maintains audit logs that record user activity within the application. The ITS.gov environment implements numerous security safeguards including intrusion detection. ITS.gov also undergoes periodic technical tests, including vulnerability scans and penetration test, to ensure the soundness of technical controls.

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?**

The Federal Reserve Bank in its role as fiscal agent for the Treasury Department has responsibility for the design, development and maintenance of the ITS.gov application. ITS entire staff must meet U.S. citizenship requirements and are subject to background investigations.

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 relies on the infrastructure for all connections required to perform ITS operations.

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

The Federal Reserve Bank 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 Kansas City Regional Financial Center provide information for use in the ITS.gov application.

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

Proper use of the data is verified with ITS general support system, Treasury, and FRB operation and security groups.