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

Fiscal Service - Privacy Impact Assessments:
https://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: Intra-governmental Payment and Collection (IPAC) System

Document Version: 1.0.0

Document Date: September 1, 2017

SYSTEM GENERAL INFORMATION:

1) System Overview:

Bureau of the Fiscal Service is responsible for maintaining effective and efficient cash management, payment and collections, accounting, and reporting systems for the federal government. IPAC is an important application in accomplishing the Fiscal Service mission. There are currently more than 270 agencies using the IPAC application. IPAC enables the transfer of funds across Federal Program Agencies (FPAs) – payment and collection transfers for goods and services (i.e., Buy-Sell transactions), fiduciary transfers (i.e., investment and borrowing transactions) and federal employee benefits data. IPAC also accepts transactions from G-Invoicing. IPAC creates settlement transactions that are sent to Central Accounting Reporting System (CARS).

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

A SORN is not required because personal identifiers are not used to retrieve individual information.

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

No

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

Yes

IPAC contains the name (First and Last Name) and government email address and governmental phone number of FPAs users.

a. Is the information about members of the public?

No

b. Is the information about employees or contractors?

Yes

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

Fiscal Service has the authority to develop and implement IPAC under regulatory code 12 U.S.C. 5018& 12 U.S.C. 391.

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
   Check all that apply:
   X **Employees**
   X **Contractors**
   __ **Taxpayers**
   __ **Others (describe)**

2) **Identify the sources of information in the system**
   Check all that apply:
   X **Employee**
   __ **Public**
   X **Federal agencies**
   __ **State and local agencies**
   __ **Third party**

   a. **What information will be collected from employees or contractors?**

      The following information about Federal Program Agencies employees, contractors, and consultants is maintained in IPAC: name (First and Last Name), governmental email address (work email address) and governmental phone number (work phone number).

   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 (FPAs) provide the data.

   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 are data collected from sources, other than Fiscal Service records, verified for accuracy?**

   IPAC does not import or export any of its Personally Identifiable Information (PII) user data.
   The users' PII data is entered by one of the following means: users enter their own PII data through the user self-registration process, or Agency Administrator (AA)/ Master Administrator (MA) may update the PII data.

b. How will data be checked for completeness?

Users check the completeness of the PII data.

c. What steps or procedures are taken to ensure the data is current?

FPAs users are responsible for updating the PII data to ensure that data is current.

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

All requirements are defined in use cases. Within each is a list describing user interface fields. These fields correspond to database entries on the back end of the IPAC application.

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?**

   The individual name and contact information collected by the system are relevant and deemed necessary for the purpose of producing IPAC services and reports.

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?**

   Not Applicable.

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

   Not Applicable.

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

   Not Applicable.

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

   No data is being consolidated.

7) **If processes are being consolidated, are the proper controls remaining in place to**

protect the data and prevent unauthorized access? (Explain)

Not Applicable.

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.)**

Personal identifiers are not used to retrieve individual 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?**

Only security reports would list information on individuals. Only authorized users are able to pull security reports and such access is limited by role and permissions.

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?**

Individuals with access to IPAC use the system only in a professional capacity to perform work-related functions. The information collected is required. The consent option does not apply.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

All data maintained by this system is retained and destroyed in accordance with the Fiscal Service File Plan. All records schedules and categories within the Fiscal Service File Plan are approved by NARA. The Retention Plan specifies that reports be retained for a minimum of 90 days.

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

All data maintained by this system is retained and destroyed in accordance with the Fiscal Service File Plan. All records schedules and categories within the Fiscal Service File Plan are approved by NARA. The Retention Plan specifies that reports be retained for a minimum of 90 days. Each report specification document states how long the report should be retained.

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?**

The application and data are replicated between a primary and backup sites. The infrastructure is responsible for replication of the data and failover to the back-up site in a contingency situation.

4) **Is the system using technologies in ways that Fiscal Service 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?**

   Not Applicable.

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?**

   None.

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

   Not Applicable.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
   X **Contractors**
   X **Users**
   __ **Managers**
   X **System Administrators**
   X **System Developers**
   __ **Others (explain)_____**

   Agency users who have appropriate levels of access and functionality may access the system. Federal Reserve Bank (FRB) operations staff have access as well.

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

IPAC limits user access through role-based security. The user provisioning system requires two individuals to grant user access.

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

IPAC access is restricted. The data accessible to users depends on their roles within the business process.

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)**

IPAC uses role-based security that applies least privilege functionality to limit user access to only what is needed to perform their duties.

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 FRB designs and develops the system acting as a fiscal agent of the U.S. Treasury. FRB employs contractors to assist in development, but contractors must meet the same requirements as bank employees (background checks, information security training, signing rules of behavior and confidentiality clauses, etc.) Privacy Act contract clauses and other regulations are met in these document

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

__yes
X **no**

If yes,

a. Explain the interface.

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

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

__yes
X **no**

If yes,

a. Check all that apply:

__Federal
__State
__ Local
__Other (explain) _____

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

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