The Bureau of the Fiscal Service

Privacy Impact Assessment

Payment Information Repository (PIR)

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: **Payment Information Repository (PIR)**

Document Version: **1.7**

Document Date: **Feb 24, 2017**

SYSTEM GENERAL INFORMATION:

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

The Payment Information Repository (PIR) is a centralized repository for federal government payment data, providing business analytics and reporting on disbursements and payments transactions to federal agencies. The system allows transaction information from payments systems to be viewed and analyzed in a single system.
The PIR is an information repository that provides information and analytics to the Financial Information Repository (FIR). The FIR allows Fiscal Service to centrally manage financial data collected in systems within Fiscal Service, including but not limited to: Revenue Collections, Delinquent Debt Collections, Intra-governmental Transfers, as well as Government-wide accounting, and Payment data.

In addition to being a repository for payment information, the PIR also serves as a key system for Non-Treasury Disbursing Offices (NTDOs) to view payment voucher data, as well as submit classification information on the payments they disburse to Government-Wide Accounting (GWA). PIR also submits DVS voucher data to CashTrack in support of Treasury's Straight Through Processing (STP) initiatives. The reporting of key financial and payment classification information to GWA and support for Treasury's Straight Through Processing (STP) initiative by providing "book to bank" matching functionality to enable STP reconcilement are supported through PIR.

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

N/A

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. The PIR contains detailed information on all government payments – including both transactional and issuance data.

b. Is the information about employees or contractors?

Yes, but only in as much as they are payees of the U.S. Government/Federal Program Agencies.

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

The following: (31 U.S.C. 321, 3301, 3325, 3327, 3328, and 3334) give Fiscal Service and the Secretary of the Treasury the legal authority and authorization for the development of the PIR.

Under 31 U.S.C. 321:

(a) The Secretary of the Treasury shall –

(1) prepare plans for improving and managing receipts of the United States Government and managing the public debt;

(2) carry out services related to finances that the Secretary is required to perform;

(3) issue warrants for money drawn on the Treasury consistent with appropriations;

(5) the Secretary of the Treasury has the general authority to "prescribe regulations that the Secretary considers best calculated to promote the public convenience and security, and to protect the Government and individuals from fraud and loss, that apply to anyone who may: (A) receive for the Government, Treasury notes, United States notes, or other Government securities; or (B) be engaged or employed in preparing and issuing those notes or securities."

Under 31 U.S.C. Sec. 3301, General duties of the Secretary of the Treasury are described:

(a) The Secretary of the Treasury shall -

(1) receive and keep public money;

(2) take receipts for money paid out by the Secretary;

(3) give receipts for money deposited in the Treasury;

(4) endorse warrants for receipts for money deposited in the Treasury;

(5) submit the accounts of the Secretary to the Comptroller General every 3 months, or more often if required by the Comptroller General; and

(6) submit to inspection at any time by the Comptroller General of money in the possession of the Secretary.

The following sections authorize:

3325 Vouchers
3326 Waiver of requirements for warrants and advances
3327 General authority to issue checks and other drafts
3328 Paying checks and drafts
3334 Cancellation and proceeds distribution of Treasury Checks

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 (Members of the General Public)

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?

PIR will not collect any information directly from taxpayers, employees, or other individuals. All data is provided through system interfaces with various applications/payment channels – such as PAM,TCIS,PACER,GWA,SAM,Easy,DVS,ITS,ASAP

b. What information will be collected from the public?

PIR does not collect any information directly from the public. All payment-related information is provided through system interfaces with various applications/payment channels such as PAM,TCIS,PACER,GWA,SAM,Easy,DVS,ITS,ASAP

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

All FPA's – both TDO and NTDO – that authorize and issue payments.

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?

Government payment channels and systems – such as Do Not Pay

3) **Accuracy, Timeliness, and Reliability**

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

The majority of the data received comes from System of Records sources, thus verification occurs at the source system. In addition, files are subject to automated validation processes. These validations ensure that information is properly formatted and meet validation rules as established by Fiscal Service and agreed upon by originating agencies. This includes activities such as balancing detail information against control records, as well as ensuring that certain/required data elements are populated appropriately.

Information from external sources comes from trusted partners such as Do Not Pay. This information is utilized to enrich the transactional data. i.e. provide context based information and is used for reporting purposes only.

b. How will data be checked for completeness?

Automated validation processes ensure that required data elements and records in incoming data files are filled according with rules established by Fiscal Service and agreed upon by originating agencies. Each file will contain control records for balancing against the contents/details of the file – for completeness. Other systematic processes will be implemented, where possible, to ensure that all files for a given day are received, verified, and processed.

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

Files are received, verified, and processed on a daily basis.

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

The data elements are described in the Input Files Specifications and Outgoing File Specifications that are contained in project document repository.

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 PIR will facilitate reporting of detailed payment information to GWA for NTDOs and will collect this data.

The PIR will act as the repository for all government payment data, and will be used to support transparency initiatives and business intelligence/analytics. Therefore, the PIR must capture as much information on government payments as possible in order to provide maximum value in this regard. Transactional data is inherently unintelligent and lacks context. Thus, traditional data warehouses or information repositories utilize additional data to bring in context-based information which can be used to discover new business insights or emerging trends that decision makers can use to optimize their business or processes.

It should be noted that the deliverables produced by these information repositories are intended to provide context or meaning to the unintelligent raw data. This process of providing context requires the need to gather additional outside facts, in order to make meaningful assertions about the data. The more facts that are gathered, the more the assertions become more statistically accurate. That being said, the use of one set of facts could lead to one conclusion, where the inclusion of an additional set of facts could lead to a different conclusion. This is the fundamental purposes of a data warehouse or information repository.

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. No individual records are kept.

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?**

The existing Fiscal Service Single Sign-On (SSO) mechanism is used for credentialing, authentication, and authorization. Additionally, within the application, data access will be secured/controlled by Agency Location Code (ALC). Workflows were designed for access approval, and all user access will be managed.

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.)**

The PIR is a data repository, ultimately designed for business intelligence and data analytics. The ways in which the data can be parsed/retrieved are many.
PIR does not use PII information to retrieve any data.

There will be a common user interface to facilitate data analysis/retrieval – with output coming in the form of dashboards and or standard file download formats. The types of data that an individual user will have access to will vary, depending upon authorizations. A user with sufficient authorization will be able to parse the data in, basically, any manner desired. PIR uses separation of duties; it contains various roles such as Helpdesk, Fiscal Service User, Agency user, ISSO.

9) **What kind of reports can be produced on individuals? What will be the use of these**

reports? Who will have access to them?

Audit and access/security/authorization reports. Only the ISSO will have access to these reports.

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?**

PIR does not collect any information directly from individuals

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

Data will be retained in accordance with Fiscal Service standards. The standard retention period for data within the PIR will be seven years – with exceptions of permanent retention where required.

Reports will be retained for 45 days prior to be deleted from the repository.

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

Disposition of data at the end of the retention period is controlled by the system, returning the space to the server operating system. PIR does not maintain a system of record on check payments, and privacy information is not documented.

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 PIR operates at a single Fiscal Service site. Application enhancements and problem changes are released through a Change Control Board process. Processing is monitored through the use of various logs, auditing and control systems.

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?**

Not applicable.

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

Auditing systems, both automated and manual, including access controls, are used to prevent unauthorized monitoring of individuals.

ACCESS TO DATA:

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

System managers, contractors, and administrators have access to the data only in as much as they are responsible for the maintenance and upkeep of the system and structures in which the data is maintained and processed.

Criteria and controls are contained in the PIR Security Plan.

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

User access is defined and controlled by role based security. Users are assigned access for the level of access needed to perform job duties based on the defined roles. Additionally, access will be restricted by ALC, with users only being able to access data related to ALCs to which they have been granted authority/access.

System Administrators have access to the data files in PIR. All transactions are written to a permanent, unalterable audit log which includes type of transaction, date/time, and user.

Managers (other than PIR end users) do not have access to production PIR. Procedures and responsibilities are contained in the PIR Rules of Behavior.

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)**

See #2 and #3 above. All Fiscal Service personnel must attend mandatory annual security and privacy training. This training includes a review of selected security and privacy procedures, regulations, and violation consequences. In addition, all personnel associated with the PIR system must sign a "Rules of Behavior" document. Those agreeing to the Rules of Behavior signify that they understand the information technology (IT) security requirements, accept the IT security requirements, and acknowledge that disciplinary action may be taken based on violation of the Rules of Behavior. This applies to all Fiscal Service employees who access IT systems as well as to all physical space housing IT systems, communications equipment, and supporting environmental control infrastructure that impact IT areas.

Additionally, the PIR will generate detailed audit logs and reports. The ISSO will have access to the logs/reports and will review them on a regular basis. These logs will contain detailed information for each access or attempted access of the system – with special emphasis on "security incidents" (i.e. automated alerts).

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, Privacy Act clauses are included in the contract. The contractor is required to adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable to agency rules and regulations.

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

__yes
_X_no

If yes,

a. Explain the interface.

The Payment Information Repository serves as a back-end to the Financial Information Repository (FIR).

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

ISSO.

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.

FPAs will be allowed access to their data in order to utilize the business intelligence tools available that provide insight into data quality and disbursements. Additionally, NTDOs will be able to validate and reconcile their payments by reviewing the bank view of payment data within PIR.

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

ISSO.