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):

https://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

Name of System: Collections Information Repository ("CIR")

Document Version: 3.1

Document Date: February 13, 2017

SYSTEM GENERAL INFORMATION:

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

CIR is a Fiscal Service-wide transaction broker, data warehouse and reporting solution that provides CIR and its trading partners with a single touch point for the exchange of all financial transaction information across all Fiscal Service collections systems. This enables Fiscal Service to normalize financial transaction reporting and standardize the availability of funds and financial information across all settlement mechanisms and collection systems. CIR greatly improves transaction information reporting which eliminates redundancies and disconnects across and between the numerous point-to-point connections currently in-place between collection agents and Federal agencies.

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

Not applicable, primary use of the system is not to search on personal identifiers.

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, there are instances when Sending Trading Partners ("STPs") have sent CIR personal information about members of the public.

b. Is the information about employees or contractors?

No. Potentially, an STP could send CIR personal information about an employee or contractor, but only as the individual is a member of the public.

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

The legal authorities applicable to this system are:

5 U.S.C 301 Departmental Regulations
31 U.S.C 321 General Authority of the Secretary
31 U.S/C Chapter 33 Depositing, keeping, and paying money

31 U.S.C 3720 Collection of Payments

DATA in the SYSTEM:

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

   Individuals and organizations that make payments to Federal government agencies, and user profile information of system users.

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

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

      None

   b. **What information will be collected from the public?**

      None directly. CIR information regarding the Public is collected from the Trading partners.

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

      Many Federal agencies have CIR user accounts and user profile information is provided .

   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?**

      STPs are the source of information in CIR. STPs are entities that provide government information to CIR.

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

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

STPs verify the accuracy of all data collected from sources other than Fiscal Service records before transmitting data to CIR.

b. **How will data be checked for completeness?**

STPs verify the completeness of all data before the data is sent to CIR.

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

STPs verify the data is current.

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

Data elements sent to CIR by STPs are described in detail in the Interface Specification document that is created for each STP.

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?**

All of the data collected by CIR is relevant and necessary for the system purpose described in the System Overview above.

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?**

N/A

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?**

CIR has data access control through the use of data type and data value data permissions that protect data from unauthorized access or use.

Every CIR user is a member of an access group and is limited to the roles, files, and trading partner data in that access group.

CIR data access control is implemented in compliance with especially Bureau's Baseline Security Requirements of *separation of duties* and *least privilege*.

CIR follows all NIST, Treasury, and Fiscal Service security requirements, policies, and procedures for access control.

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

Processes are not consolidated.

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.)**

Data is retrieved based on the information provided by STPs. Data is not retrievable by personal identifiers.

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

No reports can be produced on individuals.

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?**

CIR does not work directly with individuals. Each STP has the opportunity to decline to send information to CIR.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

Data is retained up to 1 year for transmission files from STPs depending on the retention parameter in the file profile. Reports are kept for only as long as the user is logged into CIR, however users can re-produce reports if the data is still maintained in CIR which currently can be up to 7 years.

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

No records are destroyed unless authorized under National Archives and Records Administration (NARA)-approved retention schedules and approved for destruction, in writing, by Fiscal Service Chief Counsel.

Disposition procedures are documented in the CIR Records Retention Policy.

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?**

CIR production environment has a primary and an alternate site, alternating between the Consolidation Center 3 (CC3) and the Consolidation Center 1 (CC1). In the event of a primary site failure, CIR production will be relocated to the alternate site. Data replication, along with additional backups, is used to facilitate the recovery.

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?**

N/A

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

Audit logs are built within the CIR application to track system user activity.

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

The system captures auditable records within the application and provides a traceability of user actions performed.

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

Separation of duties is enforced within the application by providing appropriate roles for the CIR user communities. Unauthorized attempts to log in to CIR are recorded within the audit log.

ACCESS TO DATA:

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

User access is based on access group, role, file, and trading partner profile data permissions on User Setup Worksheets signed by Access Group Managers. Users can also be restricted from accessing Personally Identifiable Information ("PII"). Standard Operating Procedures (SOPs) have been developed, maintained, and used by the CIR Customer Support and Operations staff.

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

A user's access is restricted by access group, role(s), function(s), and data permissions based on their business need as specified on their User Setup Worksheet. Access can be further restricted to exclude PII.

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)**

CIR maintains audit trails of user activity. Access controls are in place to enforce the separation of duties are enforced within the application. Before gaining system access, and annually thereafter, all users are required to read and agree to the CIR User Rules of Behavior.

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?**

N/A

6) **Do other systems share data or have access to the data in the system?**
_X **Yes**
__ **No**

If yes,

a. Explain the interface.

All interfaces are with systems authorized and documented in the CIR System Security Plan (SSP).

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

For each STP boarding, this role is shared by the sub-project implementation team, CIR Security Officer, CIR ISSO, and CIR Project Manager to ensure parties involved in CIR interfaces comply with Fiscal Service policies that protect the privacy rights of the affected public and employees.

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.

The other agencies will use CIR data for collections analysis and data reporting.

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

The CIR System Owner is responsible for assuring proper use of the data.

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