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: Treasury Check Information System (TCIS)

Document Version: 4.1

Document Date: 2/17/2016

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.
The Treasury Check Information System (TCIS) is a system that records and reconciles the worldwide issuance and payment of checks drawn on the U.S. Treasury. TCIS provides web-enabled access to U.S. Treasury checks and Automated Clearing House (ACH) payment data for the Bureau of the Fiscal Service (Fiscal Service), Federal Program Agencies (FPAs) and other external users through a standard web browser. TCIS allows various cancellation functions which enable the return of funds to FPAs for noncash and non-entitlement checks and processes forgery claims received from payees of U.S. Treasury checks. In addition, TCIS enables end users to initiate stop requests and request/view check images. The TCIS Treasury Check Verification Application (TCVA) provides financial institutions with a self-serve web application to verify a Treasury check has been issued, if the amounts do not match or if the item is paid.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.
FMS .002 Payment Records – Treasury/FMS
FMS .003 Claims and Inquiries on Treasury Checks and International Claimants

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?
Various statutes authorize Fiscal Service to carry out its core functions of issuing and reconciling Treasury checks. TCIS is a system that is necessary to accomplish these functions and is therefore authorized by the same statutes. They are: 31 USC sections 321, 3301, 3327, 3328 and 3334.

DATA in the SYSTEM:

1) Identify the category of individuals in the system

Check all that apply:

_ Employees
_ Contractors
X Taxpayers
X Others (describe)

Any payee associated with receiving a Treasury payment, letter, and/or supporting documentation

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

_ Employee
X Public
X Federal agencies
_ State and local agencies
X Third party

a. **What information will be collected from employees or contractors?**
Payment information is provided to Fiscal Service by agencies and may include transaction amounts, methods of payment, financial accounts information, names, addresses, taxpayer identification numbers, Treasury and agency account symbols, transaction identifiers, transaction dates, and transaction statuses.

b. **What information will be collected from the public?**
Payment information is provided to Fiscal Service by agencies and may include transaction amounts, methods of payment, financial accounts information, names, addresses, taxpayer identification numbers, Treasury and agency account symbols, transaction identifiers, transaction dates, and transaction statuses.

c. **What Federal agencies are providing data for use in the system?**
All FPAs, who are authorized to make benefit, salary, vendor, and miscellaneous payments, originate various types of information that is to be stored in TCIS. For agencies that use Treasury Disbursing Offices (TDOs), this information will come from Fiscal Service's Regional Financial Centers (RFCs) that make payments on their behalf. For agencies that use their own disbursing officers, information is provided directly from them into TCIS.

The Office of the Special Trustee for American Indians provides TCIS check issue data for checks they have disbursed.

d. **What state and local agencies are providing data for use in the system?**
N/A

e. **From what other third party sources will data be collected?**
Information on paid checks and check images (when needed) may be provided to TCIS by the Federal Reserve System. ACH payment information does not reside in TCIS, however it is viewable in TCIS. ACH payment information is located in the Payments Accounting Claims Enhanced Reconciliation (PACER) System.

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

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

The various files described above are subject to various forms of automated validations prior to processing to check for accuracy. These validations ensure that information is properly formatted. In addition, it also entails other general types of verification (e.g. ensuring valid agency information). These validation rules are primarily set by Fiscal Service.

Information related to the issuance and payment of checks and ACH payments is also subject to validation by Fiscal Service in the normal course of reconciling and adjudicating checks and ACH payments. Certain information within the system is subject to online correction by Fiscal Service employees. Field edits are performed to assure necessary information has been entered.

b. How will data be checked for completeness?

The various files described above are subject to various forms of automated validations prior to processing to check for completeness. These validations ensure that fields deemed mandatory have data within them (e.g. check symbol and serial number). These validation rules are primarily set by Fiscal Service.

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

All information provided by Fiscal Service TDOs/RFCs, Non-Treasury Disbursed Offices (NTDOs), Federal Reserve System (FRS) and Fiscal Service internal systems and end users goes through their control checks first.

TCIS performs edits on dates and duplicates when validating data it receives. Files are edited against future dates or past dates based on criteria set in the system.

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

The data elements are delineated in the Integrated View (IV), Frontier, Pega, and Transmittal Control and Disbursing Office Maintenance System (TCDOMS) user guide glossaries as well as the application help screens.

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 information collected and disseminated is relevant and necessary for Fiscal Service to fulfill its lawful mission. Fiscal Service is responsible for reconcilement of all U.S. Treasury checks disbursed world-wide and the adjudication of all claims made on U.S. Treasury checks. System profile data is needed to ensure compliance with government security laws and regulations.

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?**

The system will not derive new data or create previously unavailable data about an individual.

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?**
Data is retained in the system primarily for reconciliation and check claims purposes. Data may be consolidated for reporting purposes related to check reconcilement and check claims functions. This may include management information data.

Data related to the administrative management of the system may also be consolidated. Such information may be made available to database administrators and program representatives, including developers, as determined by the TCIS system owner as needed to investigate improvements, security breaches, or possible error resolution.

All access to any consolidated data is subject to the same restraints as set out above for non-consolidated data.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain)**
All access to any consolidated data is subject to the same restraints as set out above for non-consolidated data. Users are restricted to view only data that they have been authorized to access through user provisioning and TCIS access controls (e.g., access given by Agency Location Codes (ALCs) and read or read/write access).

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 from the system is generally retrieved by check symbol/serial number, a non-personal identifier. TCIS Integrated View (IV) only allows for the query of information by payee ID (within a date range), ACH trace number or check symbol/ serial number. The payee ID field may contain personal identifiers; however, access is limited to ensure agencies can only access their data. Fiscal Service employees may query by name or address in Frontier and Pega.
Database administrators will be able to retrieve data from databases and system administrators from audit logs by personal identifier. There are checks in place for powerful users relating to audit logs, recertification, restrictive access following the concept of least privilege and other security controls.

9) **What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
The system can provide reports based on Payee Id. Reports are created when inquiries are made by authorized personnel or the payee.

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?**
Information is only requested in response to an inquiry from an individual/claimant. An individual may decline to provide information at any time. Information is only used as required or authorized. All claimants are required to complete and sign an official Claim Form.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **What are the retention periods of data in this system? How long will the reports produced be kept?**
TCIS data and reports will be retained for 7 years, pursuant to National Archives and Records Administration (NARA) Record Retention Schedule NI-425-09-5, or as otherwise required by statute, court order, or other legal obligation.

2) **What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?**
Pursuant to court order, TCIS is not disposing Tribal Trust Litigation related data at the end of the retention period. TCIS has made a business decision to retain all data indefinitely. (The only exception is digital check images requested to resolve check reconciliation cases which are retained for sixty (60) days. However, the image may be requested through the FRS if it is subsequently needed. Other digital check images and original physical checks are currently retained indefinitely.)

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?**
TCIS has a primary operating location with a backup for contingency operations. All data is replicated to the backup location along with the creation of backup tapes at the primary location in the event data replication fails.

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.**
The information in the system is static information related to the issuance of check payments to payees. Certain personal information may be available related to their issuance (e.g., name and address) and may be used in various check after-math processes. The system does not monitor individuals.

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:
X Contractors
X Users
X 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 information within the system that is available to various parties in the normal course of business is approved by the director-level system owner of record, his/her acting manager designee, or higher senior executive.

Fiscal Service is primarily responsible for administration of Fiscal Service users. Federal Agency Administrators are primarily responsible for ensuring compliance of security procedures within their respective agencies. All requests are approved by the user's supervisor and appropriate Fiscal Service personnel prior to granting access. The system keeps detailed logs of actions taken by each employee. Access is monitored, potential security violations investigated, and appropriate remedial action taken if needed.

All Fiscal Service employees as well as FRB employees undergo a background investigation prior to employment. All contractor employees must also undergo a background investigation if they will be working on TCIS applications. TCIS users electronically sign a "Rules of Behavior" statement that delineates requirements for system use prior to accessing TCIS.

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

Fiscal Service users have access to that data and those actions needed in the normal performance of their duties. Certain actions are limited to appropriate managers/supervisors in Fiscal Service.

Agency personnel have access to data only for their own agency or have access to a subset of the data for their agency. Agency personnel primarily have inquiry access, but may be able to make certain requests for Fiscal Service action online.

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)

User roles are defined and assigned to each user when access is granted to limit system access to those capabilities required to carry out their assigned duties. Additionally, Agency Location Codes (ALCs) are assigned to the roles to limit users' access to their agencies data.

All personnel associated with and accessing the TCIS 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. It applies to all Fiscal Service employees, contractors, fiscal agents, financial agents, and subcontractor personnel who access IT systems and the facilities where Fiscal Service information is processed, transmitted, and stored as well as to all physical space housing IT systems, communications equipment, and supporting environmental control infrastructure that impact IT areas.

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

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

If yes,

a. Explain the interface.
TCIS receives information from external entities. These external entities are responsible for protecting privacy rights of information residing with them. Similarly, information that is provided to other systems have responsibility of protecting privacy rights related to the information such systems receive.

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

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.

Agencies view payment and claims information relating to U.S. Treasury checks and ACH payment information. Agencies query by a specific Check Number, by Payee ID (when agencies provide payee identification information as part of the payment request) within a range of Issue Dates, or ACH Trace Number. Agencies initiate a stop request and to request/view digital images of negotiated U.S. Treasury checks.

Agencies with legislative or delegated disbursing authority, referred to as Non-Treasury Disbursing Offices (NTDOs), as well as TDOs have the ability to:

- Track the status of the files they have submitted for processing.
- View all authorized check ranges established for their use in disbursing U.S. Treasury check payments.
- View all issue transmittals received and accepted by TCIS for a particular authorized range. This TCIS functionality is provided in the Transmittal Control and Disbursing Office Maintenance Subsystem (TCDOMS).

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

TCIS System Owner.