



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 - FMS Impact Assessments (PIA): <http://www.fms.treas.gov/pia.html>

Fiscal Service Privacy – Public Debt Impact Assessments
(PIA): http://www.treasurydirect.gov/privacy_impactassessment.htm

Document Date: August 9, 2011

Document Version: Version 2.0

Name of System: Treasury Receivable, Accounting and Collection System (TRACS)

SYSTEM GENERAL INFORMATION:

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

TRACS is a Tier II mission supportive application system that is designed to support the FMS Check Resolution Division. TRACS, which is a minor application, supports the FMS Payment business line as a debt recovery and accounting system. TRACS utilizes DB2 and associated support applications on the Mainframe to provide accounting financial reporting, debt billing and collection activity associated with the U.S. Treasury Check Claims process. TRACS assumes the responsibility for the accounting and reporting of Check Reclamations (REC), Unavailable Check Cancellations (UCC), Limited Payability Cancellations LPC), and Payments over Cancellation (POC).

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

.002 Payment Records

.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.

no

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

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 FMS to carry out its core functions of issuing and reconciling Treasury checks. TRACS 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
- Taxpayers
- Others (describe)

2) Identify the sources of information in the system

Check all that apply:

- Employee
- Public
- Federal agencies
- State and local agencies
- Third party

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

Payment information from the public may include transaction amounts, methods of payment, financial accounts information, names, addresses, taxpayer identification numbers, agencies authorizing the payment, Treasury and agency account symbols, transaction identifiers, transaction dates, and transaction statuses. Various administrative information is also associated with the system, including employee usernames and passwords.

b. What information will be collected from the public?

Payment information from the public may include transaction amounts, methods of payment, financial accounts information, names, addresses, taxpayer identification numbers, agencies authorizing the payment, Treasury and agency account symbols, transaction identifiers, transaction dates, and transaction statuses. Various administrative information is also associated with the system, including employee usernames and passwords.

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

All FPAs and Non Treasury Disbursing Office (NTDO), who are authorized to make benefit, salary, vendor, and miscellaneous payments by Treasury check.

d. What State and local agencies are providing data for use in the system?

The Office of the Special Trustee for American Indians (Disbursing Office Symbol 4844) provides TCIS check issue data for checks they have disbursed. TCIS provides check information to TRACS.

e. From what other third party sources will data be collected?

N/A

3) Accuracy, Timeliness, and Reliability

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

The various files described above will be 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 FMS.

Information related to the issuance and payment of check payments is also subject to validation by FMS in the normal course of reconciling and adjudicating check payments. Certain information within the system will be subject to online correction by FMS 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 will be 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 serial number). These validation rules are primarily set by FMS.

Authentication information provided by end-users is subject to browser-based and server-based error checking to ensure that the information is complete.

Control totals follow NIST guidelines.

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

Yes, the data is current. System checks on document number and confirmation date of documents including Payment Over Cancellation (POC), Unavailable Check Cancellation (UCC), Limited Payability Cancellation (LPC), and Limited Payability Declination (LPD)

All information provided by FMS TDOs/RFCs, NTDOs, FRS and FMS internal systems and end users goes through their own control checks first.

TCIS performs edits when validating data it receives. Files are edited against future dates or past dates based on criteria set in the system prior to transfer of data to TRACS.

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

Yes, the TRACS data dictionary is the document that stores all data elements related to TRACS. The dictionary reflects all data elements alphabetically by name, a description, comments, data type, maximum field length, and business name for each data element.

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?

Yes. All information collected and disseminated is relevant and necessary for FMS to fulfill its lawful mission. FMS is responsible for reconciliation 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 through aggregation from the information collected.

3) Will the new data be placed in the individual's record?

N/A. The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

N/A. The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

N/A. The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

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

Data will be retained in the system primarily for check claims accounting purposes. Data may be consolidated for reporting purposes related to check claims accounting 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 TRACS 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 TRACS access controls (e.g., access given by 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. You cannot query by name or address.

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, access to least privileged and other security controls.

The effects are mitigated as described above.

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

N/A

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

Security is of utmost importance and access is controlled on a need to know basis. Management decides who has access to what data. FMS collects only the information necessary to process a claim. A claim cannot be processed without that information. Providing the information is mandatory.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

TRACS will follow appropriate data retention planning, NARA and legal requirements when applicable. The normal retention period for the data in the system is seven years. However, FMS is currently retaining all data in this system indefinitely, due to pending litigation.

TRACS will follow retention schedule N1-425-01-4. This is a pending schedule which allows for the transfer of paper records to a Federal Records Center; it cannot be used to destroy/delete records

NARA will not approve the schedule (N1-425-01-4), until litigation issues involving the records are resolved.

From (N1-425-01-4), item 1

A. Inputs: Delete input files 30 days after input and verification

B. Master File— (1) Individual Indian Monies (IIM) records: Delete from database and index when 20 years old

(2) Non-IIM (all other) records: Delete from database and index when 7 years old

C. Outputs— (1) Output files to other systems: Delete 30 days after output

(2) Electronic versions of output reports: Delete from data base when 20 years old (3) Paper versions of output reports: Destroy when no longer needed for agency business

D. Documentation: Maintain for life of system plus 3 years

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

By federal court order, FMS is not eliminating any data from this system and does not plan to do so in the foreseeable future.

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?

N/A – TRACS is operated from only one site.

4) Is the system using technologies in ways that FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Authentication is provided by SecurID, Network Security with password and User ID.

5) How does the use of this technology affect employee or public privacy?

The use of TRACS allows for more efficient retrieval and processing of data needed in the routine course of business. Some of this data may be personal in nature. However, procedures surrounding its care and use as described earlier will not change.

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 identify or monitor individuals.

For security purposes, to safeguard information contained in the system, software will be employed to monitor access to the system. A log will kept of valid and invalid attempts to gain access to the system; it may include date, user id, password, and log-on/log-off-related information. Audit log information has limited access. TRACS will comply with FMS standards.

For administrative purposes, the system will also retain information related to the identity of employees that have made changes or completed processes within the system in the normal course of business.

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

TRACS does not monitor individuals.

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

Network security with password and User ID ensures that data retrieved is data necessary in the routine course of business and the public/employee's privacy is protected.

TRACS will not actively monitor individuals or groups. For security purposes, to safeguard information contained in the system, software will be employed to monitor access to the system. A log will kept of valid and invalid attempts to gain access to the system; it may include date, user id, password, and log-on/log-off-related information. Audit log information has limited access. TRACS will comply with FMS standards.

ACCESS TO DATA:

1) Who will have access to the data in the system?

Check all that apply:

- Contractors**
- Users**
- Managers**
- 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?

Information that is collected and used with respect to payees is necessary and relevant to the check after-math processes or other legally mandated or authorized purposes. The information within the system that will be 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. FMS receives much of the information related to this system from program agencies via TCIS, but also receives it from other sources as well in the course of carrying out its mission related to check after-math processes. These sources include Federal Reserve banks and payees.

FMS will be primarily responsible for administration of FMS users. Federal agency administrators will be primarily responsible for ensuring compliance of security procedures within their respective agencies. Documentation will detail who may have what level of access in the system. All access requests must be placed in writing within a formal access control system. All requests will be

approved by appropriate personnel prior to granting access. The system will keep detailed logs of actions taken by each employee.

Interfacing files with the system come and leave the system via secure means for sensitive but unclassified data.

All FMS employees as well as Federal Reserve Bank (FRB) employees undergo a background investigation prior to employment. All contractor employees must also undergo a background investigation if they will be working on the TRACS application. All FMS personnel sign a "Rules of Behavior" statement that delineates requirements for system use.

Access to data by an end-user requires that an end-user be authenticated using a TRACS username and password. In addition, authentication is provided by a user gaining access from a trusted site at an agency over a T-1 line or Citrix.

In addition to those referenced, the above is part of various business and security requirements, standard operating procedures, and in agreements. These requirements and others are delineated in several documents, including the Privacy Act of 1974, as amended, the FMS Security Manual (last updated 4/21/05), the FMS Privacy Act Overview policy (last updated 10/7/04), the FMS Sensitive Information Security Controls policy (last updated 7/29/04), and the FMS Sensitive Information Control standard (last updated 7/29/04).

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

FMS users will have access to that data and those actions needed in the normal performance of their duties. Certain actions will be limited to appropriate supervisors in FMS.

Agency personnel will have access to data only for their own agency or have access to a subset of the data for their agency. SSA personnel will have query access.

TRACS database administrators will have access to database information. This is required for monitoring unauthorized access and/or use of the system.

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)

All FMS personnel must attend mandatory annual security training. This training includes a review of selected security procedures. All personnel associated with the TRACS system must sign a "Rules of Behavior" document. Those agreeing to the Rules of Behavior signify that they understand the 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 FMS employees, contractors, fiscal agents, financial agents, and subcontractor personnel who access IT systems and the facilities where FMS 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. Privacy Act contract clauses were inserted into their contracts.

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

yes

no

If yes,

- a. **Explain the interface.**

As previously noted, TRACS 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.**

AC area Privacy Act Liaison

Senior Official for Privacy

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

yes

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.**

External agency will have the ability to query data that they have check number information for, from their agency. The information is used to assist their agency customers in the Check Claim and Limited Payability process.

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

The external agency management and each of their users are responsible for proper use of data. Each user signs a TRACS Rules of Behavior that includes how information is handled.