U.S. Department of the Treasury
Financial Management Service (FMS)
Privacy Impact Assessment (PIA)

System Name: Treasury Receivable, Accounting and Collection System
Unique Identifier: TRACS

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) **Does this system contain any information about individuals?**

Yes

a. **Is this information identifiable to the individual'[1]?** (*If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the PIA does not have to be completed.*)

Yes

b. **Is the information about individual members of the public?** (*If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security Certification and Accreditation (C&A) documentation*).

Yes

c. **Is the information about employees?** (*If YES and there is no information about members of the public, the PIA is required for the FMS IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation*).

No - Employees only included as members of the public

2) **What is the purpose of the system/application?**

TRACS is a "TIER II" mission supportive application system that is designed to

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

support FPD. TRACS, which is a minor application, supports the FMS payments 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, unavailable check cancellation (UCC), limited payability cancellation (LPC), and payments over cancellation (POC).

3) **What legal authority authorizes the purchase or development of this system/application?**

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.

B. DATA in the SYSTEM:

1) **What categories of individuals are covered in the system?**

Any payee associated with receiving a Treasury check.

2) **What are the sources of the information in the system?**

TRACS sources are listed below: The system is not designed to produce reports on individuals. Division management can get case workload statistical information.

a. **Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Information may come from the individual claimant, but mostly it is from other sources as listed above. The information to be stored in the system comes from a number of entities. Check issuance and cancellation information is provided by Treasury disbursing offices (TDOs) and NTDOs. Paid check information is received from the Federal Reserve bank (FRB). Information from payees may also be stored in the system. Check payments are for various types of payments including benefit, salary, vendor, and miscellaneous payments.

b. **What Federal Agencies are providing data for use in the system?**

All Federal Program Agencies (FPA) who are authorized to make benefit, salary, vendor, and miscellaneous payments by Treasury check.

c. What Tribal, 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 and paper UCC documents. TCIS provides check information to TRACS.

d. From what other third party sources is the data collected?

N/A

e. What information will be collected from the employee and 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.

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. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Yes, the data is current. The system checks on document number and confirmation date of documents including POC, UCC, LPC, and limited payability declination.

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. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, the data dictionary is the document that stores all data elements related to TRACS.

C. <u>ATTRIBUTES OF THE DATA:</u>

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and 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/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, 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 is the data to be retrieved? Can it be retrieved by personal identifier? If yes, explain. How are the effects to be mitigated?**

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 kinds 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), and how individuals can 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.

D. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

N/A

2) **What are the retention periods of data in this system?**

TRACS will follow appropriate data retention planning, NARA, and legal requirements when applicable. The normal retention period for the data in the system is 7 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:

- Inputs: Delete input files 30 days after input and verification

- 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.

- 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

- Documentation: Maintain for life of system plus 3 years

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the 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.

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 public/employee 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.

No.

7) What kinds of information are collected as a function of the monitoring of individuals?

NA

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

NA

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Pursuant to the Privacy Act of 1974, as amended, 5 U.S.C. 552a, FMS has established the following applicable system of record numbers and titles.

FMS .002 – Payment Issue Records for Regular Recurring Benefit Payments

FMS .016 - Payment Records for Other Than Regular Recurring Benefit Payments

FMS .003 - Claims and Inquiry Records on Treasury Check and International Claimants

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

N/A - Currently, there are no plans to modify TRACS.

E. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (*E.g., contractors, users, managers, system administrators, developers, tribes, other*)

Information in the system is generally available to FMS employees according to the authorities granted to them. Personnel associated with other Federal Agencies also have access to information for their particular agency. The information of one agency may not be viewed by another agency. In addition, data will be available to various FMS and FRB personnel and any of their contractors in the performance of their normal duties.

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

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.

All FMS 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 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 agreements. These requirements and othe rs are delineated in several documents: The Privacy Act of 1974, as amended; the FMS Security Manual (last updated 4/21/05); the FMS Privacy Act Overview policy (last updatedl0/7/04); 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. Social Security Administration 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?**

All FMS personnel must attend mandatory annual security training. All personnel associated with TRACS must sign a "Rules of Behavior" document.

5) **Are contractors involved with the design and development of the system**

and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and 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? If yes, explain.**

TRACS receives information from external entities. These external entities are responsible for protecting privacy rights of information residing with them. Similarly, external entities that are provided information to their systems are responsible for protecting privacy rights related to the information.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The TRACS system owner.

8) **Will other agencies share data or have access to the data in this system (Federal, state, local, other (e.g., tribal))?**

Yes, other Federal Agencies also have access to information for their particular agency. The information of one agency (or subset thereof) may not be viewed by another agency (or subset thereof).

9) **How will the data be used by the other agency?**

As mentioned above, much of the information within the system is often that which was originated by the Federal Agencies and is resident in their systems. Data will normally only be disclosed to those agencies that originated payments that led to reconcilement and adjudication information.

10) **Who is responsible for assuring proper use of the data?**
The system owner