US Department of the Treasury
Financial Management Service
Payment Management
Check Resolution Division
Office of Trust Fund Management (OTFM) Activity Tracking System (OATS)

Privacy Impact Assessment (PIA)

Name of System: OATS
Bureau: Financial Management Service
Payment Management
Check Resolution Division

A. SYSTEM APPLICATION/GENERAL INFORMATION:

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

   a. Is this information identifiable to the individual[1]? Yes
   (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.)

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

   c. Is the information about employees? No
   - Employees only included as members of the public
   (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).

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

[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).

OATS is a "TIER II" mission supportive application system that is designed to support the FMS Check Resolution Division. OATS, which is a Major Application, supports the FMS Payments business line. OATS provides the storage and retrieval of information for checks issued by the Office of Trust Fund Management (OTFM) and checks negotiated through the Federal Reserve System (FRS).

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

The OTFM Activity Tracking System was developed as a result of stipulations made by Commissioner Dick Gregg on July 6, 1999 as part of the *Cobell et al. v. Babbitt et al.* litigation. Two stipulations, dealing with both negotiated and unnegotiated checks, required that new system be built to provide the predicate information (check symbol and serial number) needed to conduct searches in the old Check Payment & Reconciliation (CP&R) system, which was replaced by the Treasury Check Information System (TCIS).

B. DATA in the SYSTEM:

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

Payees receiving Bureau of Indian Affair payments for Individual Indian Money (IIM) accounts.

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

OTFM sends payments issued by the OTFM. The FRS sends negotiated checks. The PACER On-Line application sends Electronic Funds Transfer (EFT) payment data.

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?

Check issued payments come from OTFM. Checks negotiated through the FRS come from the FRS. Electronic payment information comes from the FMS PACER On-line application.

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

Department of Interior, Bureau of Indian Affairs, is providing data.

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. Issue transmittals generally include the issue transmittal number, accounting date, check symbol number, check serial number, issue date, issue amount, payee ID, Agency Location Code (ALC), appropriation code (Treasury Account Symbol) and the item count and dollar amount of all the individual records contained in the transmittal. The format for issue transmittals received from the Office of the Special Trustee for American Indians has two additional data elements from the standard issue transmittal format; the payee's last name and zip code. TCIS transfers this data to OATS.

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, financial accounts information, names, taxpayer identification numbers, agencies authorizing the payment, Treasury and agency account symbols, transaction identifiers, and transaction dates. Various administrative information is also associated with the system, including payee id.

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 check payments. 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.

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).

The data is current. All information provided by OTFM, FRS, and FMS PACER On-Line internal systems goes through their control checks first.

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

Yes, the data elements are documented in the OATS user guide.

C. ATTRIBUTES OF THE DATA:

1) 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 reconcilement of all U.S. Treasury checks disbursed world-wide and for storage and retrieval of information for checks issued by OTFM and checks negotiated through the FRS.

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, and 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/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 the storage and retrieval of information for checks issued by OTFM and checks negotiated through the FRS. No data is being consolidated.

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

N/A. No processes are being consolidated.

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 payee (last) name or payee ID. The payee ID is an OTFM unique identifier. The OTFM's payee ID identifies the tribe (3 digits), type of payment (alpha character) and individual (by 6-digit number). OATS only has three internal users who use the system on an "as needed basis".

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.

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.)

The individual does not have the opportunity to decline.

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 – OATS is operated from only one site.

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

OATS 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.

OATS 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

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 the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No.

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

The use of this technology 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). 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. OATS will comply with FMS standards.

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

OATS does not monitor individuals.

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

OATS will not actively monitor individuals or groups.

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 number and titles.

Payment Issue Records for Regular Recurring Benefit Payments—Treasury/FMS .002

Payment Records for Other Than Regular Recurring Benefit Payments—Treasury/FMS .016

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 OATS.

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 available to three FMS employees, with "read-only" access to the data in the system. Employees are counseled that they may only view information available to them on a "need-to-know" basis in the performance of their duties.

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

Information collected is used for storage and retrieval for checks issued by OTFM and OTFM checks negotiated through the FRS. The data is used for 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.

Procedures will be in place for the system, and FMS will be primarily responsible for administration of FMS users. 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 undergo a background investigation prior to employment. 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 an OATS username and password.

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.

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.

OATS 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. This training includes a review of selected security procedures. All personnel associated with the OATS 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) **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?

No.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

As previously noted, OATS receives information from TCIS and PACER On-Line, both FMS applications. They follow the same responsibility for protecting privacy rights of information residing with them as the OATS application. OATS receives data from Office Trust Fund Management (OTFM) Data Entry System (ODES). ODES does not have access to OATS. OATS does not share data with any system.

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

The OATS system owner.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

OTFM shares data with TCIS, and TCIS sends the data to OATS. OTFM does not have access to the data in the OATS system.

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 agency and is resident in their systems. Data is not disclosed to the agency.

10) Who is responsible for assuring proper use of the data?

The OATS system owner and the bureau head.