Financial Management Service

Privacy Impact Assessment

The Financial Management Service (FMS) Mission is to provide central payment services to Federal Program Agencies, operate the federal government's collections and deposit systems, provide government-wide accounting and reporting services, and manage the collection of delinquent debt owed to the government.

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

Document Date: June 8, 2011

Document Version: 1.8

Name of System: Treasury Check Information System (TCIS)

SYSTEM GENERAL INFORMATION:

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

TCIS is a "TIER II" mission supportive application 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 ACH payment data for FMS, 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. In addition, TCIS' Treasury Check Verification Application (TCVA) provides financial institutions with a self-serve web application to verify that 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.

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

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

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 FMS 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
__ Taxpayers
_X_ Others (describe)
Any payee associated with receiving a U. S. Treasury check.

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

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

Payment information is provided to FMS 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 FMS 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 TDOs, this information will come from FMS' RFCs that make payments on their behalf. For agencies that use their

own disbursing officers, information is provided directly from them into TCIS. In addition, some data also will come into TCIS via other FMS systems.

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?

Information on paid checks and check images (when needed) will also 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 PACER.

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 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 FMS.

Information related to the issuance and payment of checks and ACH payments is also subject to validation by FMS in the normal course of reconciling and adjudicating checks and ACH payments. Certain information within the system is 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 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 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?

All information provided by FMS TDOs/RFCs, NTDOs, FRS and FMS 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 essentially delineated in the IV, Frontier, Pega , and 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 FMS to fulfill its lawful mission. FMS 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 does 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 does 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 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 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 # or check symbol/ serial number. You can query by name or address in Frontier and Pega that is used only by FMS' employees. However, the social security number is commonly used as the payee ID field. This is mitigated by the fact that those agencies accessing the system can only see their own data.

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?

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., 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 provided 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 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.

TCIS 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. (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 operates from one site located in Dallas, TX.. The Integrated View module is located from Kansas City, MO. IV is a query function of the system to access and display information contained in CP&R (archived data), PACER on-line, and TCIS.

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

TCIS uses PKI level II authentication for all Internet users.

5) **How does the use of this technology affect employee or public 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 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. TCIS complies with FMS standards.

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

The use of cookies is minimized and, when actually used, the session cookies are stored in RAM and will not be written to the user's computer.

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

TCIS does not monitor individuals.

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

The system does not actively monitor individuals or groups.

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
_X_ Others (explain)_____

Information in the system is generally available to FMS employees according to the authorities granted to them. Employees are counseled that they may only view information available to them on a "need-to-know" basis in the performance of their duties. 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 is 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?**

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 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. FMS receives much of the information related to this system from program agencies, 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 is primarily responsible for administration of FMS users. Federal Agency Administrators are 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. The Treasury Web Applications Infrastructure (TWAI) as well as designated FMS employees will monitor access, investigate potential security violations, and take appropriate remedial action if needed.

Interfacing files with the system come and leave the system via secure means for sensitive but unclassified data. There is no change in the level of security for interfacing files.

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 TCIS 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 TCIS username and password. In addition, two-factor authentication is provided by a PKI or a user gaining access from a trusted site at an agency over a T-1 line.

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 updated10/7/04), 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 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 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 FMS action online.

TCIS database administrators have access to database information. Program managers at FMS, FRB, and TWAI as well as system administrators (including the FMS application information system security officer, FRB personnel, and TWAI personnel) will have access to audit logs of actions taken within the system. 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 take a mandatory Cyber Security Awareness annual security training course. This training includes a review of selected security

procedures. All personnel associated with the TCIS 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

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

If yes,

As previously noted, 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.

a. Explain the interface.

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

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:
__Federal
__State
__ Local
_X_Other (explain) _____

Procedures are in place for the system. FMS is primarily responsible for administration of FMS users. Federal agency administrators are primarily responsible for ensuring compliance of security procedures within their respective agencies. Profile information is created by federal agency authentication administrators. Documentation details who may have what level of access in the system. All access requests are placed in writing within a formal access control system. All requests are approved by appropriate personnel prior to granting access. The TWAI as well as designated FMS employees monitor access, investigate potential security violations, and take appropriate remedial action if needed.

Access to data by an end-user requires that an end-user be authenticated using a TCIS username and password. There are two authorities for system security—one is from a platform perspective and the other is from an application perspective. Security procedures are well documented by the TWAI.

It should be noted that much of the information within the system is often that which was originated by the federal agencies and is resident in their systems. Data is normally only disclosed to those agencies that originated payments that led to reconcilement and adjudication information. Any other disclosures will be made only in accordance with the provisions of 26 USC 6103 (restricting the disclosure of tax return information), 5 USC 552a (the Privacy Act) and 18 USC 1905 (the Trade Secrets Act), and other applicable laws and will be made using the procedures outlined above.

b. Explain how the data will be used by the other agencies.

Personnel associated with 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).

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.

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

The TCIS system owner has responsibility for ensuring compliance.

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