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: **April 26, 2011**

Name of System/Application: **Judgment Fund Internet Claim System (JFICS)**

System Overview:

Congress enacted a permanent, indefinite appropriation - the ***Judgment Fund*** for payment of judgments not otherwise provided for in 1956. In 1961, Congress modified the law to allow payments from the Judgment Fund appropriation in cases involving compromise settlements, actual litigation or imminent litigation, involving the Department of Justice (DOJ). In addition, Congress has authorized payments from the Judgment Fund appropriation for paying many Federal agency administrative settlements without a lawsuit. As a permanent indefinite appropriation, the Judgment Fund operates independently of the normal congressional authorization process. It has no fiscal year limitations, no appropriation amount limitations, and no judgment or settlement amount limitations. In effect, it is a standing authority to draw money from the general fund (General Fund) of the United States Treasury (Treasury). However, it is important to remember that the Judgment Fund Branch (JFB) does not pay judgments; it only certifies them for payment.

Payments from the Judgment Fund appropriations require certification, a function currently performed by the Judgment Fund Branch, Financial Management Service (FMS), a bureau within the Department of the Treasury. The primary responsibility of the JFB is to determine whether the proper source of funds for the payment of claims is the Judgment Fund or whether the source is otherwise provided for by law or statute. In the course of certification, the JFB must also confirm the finality of the judgment or award. The Judgment Fund Internet Claims System (JFICS) allows for electronic tracking of the claims submission. The database is updated to reflect the current status based on user input. The JFICS improves customer service and allows efficient processing of claims. All claims through JFICS are subjected to the approval process designed within the workflows of the system. Once a claim has been approved for payment, the payment information is uploaded to the FASD Oracle. JFICS database creates a file to be uploaded to Oracle which is referred to as the Transaction Layout File. Oracle is the accounting system for the Judgment Fund payments. Once payments have been issued a Confirmation File is sent from Oracle to JFICS.

System of Records Notice (SORN): .003 Claims and Inquiries on Treasury Checks and International Claimants

SYSTEM APPLICATION/GENERAL INFORMATION:

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

a. Is the information about individual members of the public? YES

b. Is the information about employees or contractors? NO

DATA in the SYSTEM:

1) **Categories of individuals covered in the system**
Check all that apply:

_X_ Employees
__ Contractors
_X_ Taxpayers
_X_ Others (describe)—Claimants and their attorneys associated with Judgment Fund claims

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

_x_ Employee
__ Public
_X_ Federal agencies
__ State and local agencies
__ Third party sources

a. What Federal agencies are providing data for use in the system? Only authorized FPAs can submit a claim for payment to the Judgment Fund.

b. What State and local agencies are providing data for use in the system? None

c. From what other third party sources will data be collected? None

d. What information will be collected from employees or contractors? The claim information includes the name(s) of claimants, as well as the SSNs/EINs, and addresses or banking information for claimants or person receiving payments. In addition, information related to claimant attorneys is collected.

e. What information will be collected from the public? None

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

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

Verification for data accuracy is achieved in several ways. Presently, the data is verified for accuracy by comparing the system data with the supporting documentation. The system contains a reconciliation procedure that checks totals entered in the system against the total payments anticipated by the agency. If an agency submits incorrect RTN or address information, the financial institution or the U.S. Postal Service will return a misdirected payment. In the future, software will be used to ensure the validity of RTN data.

b. How will data be checked for completeness? Edits at the time of on-line data submission will ensure that all required information is provided.

c. What steps or procedures are taken to ensure the data is current and not out-of-date? Judgment Fund payments are typically not recurring payments. Therefore, each payment is made based on new information entered into the system for that specific purpose.

d. In what document(s) are the data elements described in detail? Refer to applicable sections of the project documentation, i.e., JFICS System Security Plan, JFICS System Contingency Plan

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? The use of the data is relevant and necessary. The data is used to track the submission of cases to the JFB. The cases have to be analyzed for approval and subsequent certification of payment from the Judgment Fund.

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? Not applicable

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

5) How will the new data be verified for relevance and accuracy? Not applicable

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use? Not applicable

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain.) Not applicable

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 may be retrieved by means of a personal identifier, which may include a name, system-assigned number, or SSN.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them? The system is not designed to produce reports on individuals. Branch and division management can get case workload statistical information. The system generates automated audit report queries monthly for deleted cases and audit logs for SVS for user actions relating to tables related to PII and SBU activity.

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 can individuals grant consent.) The information is provided to us by FPAs. Such information must be provided if an individual/company wants to receive a payment for a claim.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

What are the retention periods of data in this system? How long will the reports produced be kept? In accordance with the National Archives and Records Administration (NARA) schedule for the records related to this system (Pending schedule N1-425-01-04), data will be retained in JFICS for seven (7) years. Currently, any FMS records that are proposed for destruction must be approved in advance, and in writing, by the FMS Assistant Commissioner for Management and the FMS Chief Counsel, to ensure compliance with NARA disposition schedules and any record retention orders to which FMS is subject. The FMS Chief Counsel outlined this process in a memorandum to the FMS Assistant Commissioners, dated March 7, 2000.

1) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented? This is discussed above.

2) If the system is operated in more than one site, how will consistent use of the system and data be maintained at all sites? Not applicable.

3) Is the system using technologies in ways that the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)? No

4) How does the use of this technology affect employee or public privacy? Not applicable

5) Will this system provide the capability to identify, locate, and monitor individuals? NO.

6) What kinds of information are collected as a function of the monitoring of individuals? An audit trail will be captured for each transaction that adds, deletes or modifies any information. The audit trail will include the UserID of the person performing the transaction.

7) What controls will be used to prevent unauthorized monitoring? Access to the audit logs is limited to authorized individuals within the Information Resources (IR) organization. Requests for review of the data must come from management-level personnel.

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
__X Others (explain)_____Data will be accessible by the JFB staff, the JFICS database administrator at FMS, and by certain IR Development Staff and authorized contractors working in IR. It will also be accessible to authorized users at the specified agency that submitted each claim.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented? JFICS defines access control policy, groups and individual user permissions based on least privilege. Access and permissions are restricted to the approved domain. Granting of initial or change in access or permissions must be accomplished in writing and approved by the Judgment Fund Manager.

3) Will users have access to all data on the system or will the user's access be restricted? Explain. User access will be restricted. FPA users will be restricted to accessing only their FPA data. Internal users will have the level of access needed to perform their duties. Users with administrative privileges are restricted to the minimum necessary and all action are monitored and recorded in various system logs and audit trails.

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) The JFICS application contains an access control module. Users are defined in an LDAP user directory. Roles have been defined and are issued to grant access to each individual commensurate with the user's need. Specific roles have been defined for administrators, analysts of various agencies, and users who need to enter specific transactions in JFICS. Active auditing of system and application access and the use of individual UserIDs allow enforcement of individual accountability and traceability of user actions. Rules of Behavior (ROB) are signed by users before gaining access to the system. ROB will be automated by January 2012.

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? No

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

_X_yes
__no

If yes,

a. Explain the interface. JFICS data is uploaded into Oracle, which interfaces with SPS. This data is also shared with POL and TOP.

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

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) _____FPAs including Dept. of Justice____________

b. Explain how the data will be used by the other agencies. To track cases paid out of the Judgment Fund and to also receive summary level information on payment/case type.

c. Identify the role responsible for assuring proper use of the data. To track cases they have submitted. Approving Users and Reviewer and Manager roles

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