US Department of the Treasury
Financial Management Service (FMS)
Privacy Impact Assessment (PIA)

Name of Project: Judgment Fund Rapid Application Development System
Project's Unique ID: JFRAD

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

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

   JFRAD is a mission supportive application system that is designed to support the FMS Judgment Fund Branch (JFB) in administering the Judgment Fund System (JFS). JFRAD will be used by JFB to collect information related to claims submitted for payment out of JFS, to review such claims for proper payment out of JFS, and for authorizing the payments. The system is being developed in a series of releases. The first release will allow the online submission of claims data by a very limited number of users at one agency Subsequent releases will increase the functionality of JFRAD to include internal claims processing.

[1] "Identifiable Form" – According to OMB 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.)

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

Congress established JFS which is a permanent, indefinite appropriation to pay certain judicially and administratively ordered monetary awards against the United States and to pay the amounts owed under compromise agreements negotiated by the U.S. Department of Justice in settlement of claims arising under actual or imminent litigation. In general to qualify for payment from the fund, awards must be final, must require payment of specific sums of money awarded against the United States under one of the authorities specified in 31 U.S.C. § 1304(a)(3), and may not legally be payable from any other source of funds.

Pursuant to Public Law 104-53 (November 19, 1995), the fund function was transferred from the Government Accounting Office to the Office of Management and Budget (OMB). The OMB director delegated this responsibility to Treasury, FMS.

B. DATA in the SYSTEM:

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

Claimants and their attorneys associated with JFS claims.

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

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?**

The source of the information is Federal Program Agencies (FPA) or the Department of Justice.

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

Only authorized FPA can submit a claim for payment out of JFS.

c. **What Tribal, State and local agencies are providing data for use in the system?**

None

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

None

e. **What information will be collected from the employee and the public?**

The claim information includes the name(s) of claimants as well as the social security number (SSN)/employer identification number (EIN) and addresses or banking information for claimants or persons receiving payments. In addition, information related to claimant attorneys is collected.

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

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

Presently, the data is verified for accuracy by comparing the system data with the supporting documentation. 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. **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 submitting agency is responsible for ensuring that address or banking information is current at the time it is provided.

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

Yes, in the security plan, user manual, and the project design document.

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?**

NA

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

NA

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

NA

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

NA

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

NA

8) **How is the data to be retrieved? Does a personal identifier retrieve the data? (***If yes, explain and list the identifiers that will be used to retrieve information on the individual***.)**

Yes, data may be retrieved by means of a personal identifier which may include a name or system-assigned number. Eventually, data will be retrievable by 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?**

No reports can be produced on individuals.

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 information is provided to us by FPAs. Such information must be provided if the person wants to receive a payment for a claim.

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?**

   NA

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

   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 JFRAD for 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.

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?**

   This is discussed above.

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?**

   NA

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

   Internal users of the system may access data with the use of a unique UserID and password.

7) **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.

8) **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.

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

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

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

NA.

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*)

Data will be accessible by JFB, the database administrator, certain development staff, and authorized contractors. It will also be accessible to authorized users at the specific 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?**

JFRAD defines access control policy, groups, and individual user permissions based on least privileged. 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 JFS 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 actions 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)*

JFRAD contains an access control module. Users are defined in an LDAP user directory. Roles have been defined and are used 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 JFRAD. 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 are signed by users before gaining access to the system.

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.**

Yes. JFRAD provides input data for JFS via data entry. JFS data is uploaded into Momentum which interfaces with the Secure Payment System. This data is also shared with PACER On-Line and the Treasury Offset Program.

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

Information owner and system manager

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

FPAs that submit cases including the Department of Justice will have access to the data for cases they submit.

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

They will be able to use it for the tracking of cases that they have submitted.

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

The branch manager, the ISSO, and/or the alternate ISSO