U.S. Department of the Treasury
Financial Management Service
Financial Operations
Financial Accounting and Services Division
Judgment Fund Branch
JFS System
Privacy Impact Assessment (PIA)

Name of Project: JFS System
Bureaus: Financial Management Service (FMS)
Financial Operations (FO)
Financial Accounting and Services Division (FASD)
Judgment Fund Branch (JFB)

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- JFS Information Systems Security Officer (ISSO)
- All Signatories to the JFS PIA
- FMS Privacy Act Liaison
- FO Audit Liaison

Do not email the approved PIA directly to the Office of Management and Budget (OMB) email address identified on the Exhibit 300 form. One transmission will be sent by the FMS Privacy Act Liaison.

Also refer to the signature approval page at the end of this document.

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

[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).

b. Is the information about individual members of the public?

Yes

c. Is the information about employees?

Yes

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

The JFS system is a mission supportive application system that is designed to support the FMS Judgment Fund Branch ("JFB") in administering the Judgment Fund. JFS is used by the JFB to collect information related to claims submitted for payment out of the Judgment Fund, to review such claims for proper payment out of the Judgment Fund, and for authorizing the payments.

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

Congress established the Judgment Fund, 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 GAO to the Office of Management and Budget (OMB). The Director, OMB, 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 Judgment Fund claims.

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

Federal Program Agencies (FPAs) and the Department of Justice submit claims for payment out of the Judgment Fund. The information is submitted via the Internet or on paper. The claim information includes the name(s) of claimants, as well as the SSNs/TINs, and addresses or banking information for claimants receiving payments. In addition, information related to claimant attorneys is collected.

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 the FPA or the Department of Justice.

b. What Federal agencies are providing data for use in the system? Any agency can submit a claim for payment out of the Judgment Fund.

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 SSNs/EINs, 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, there is no "verification" for accuracy since the agency mails the claims submissions and JFB cannot check the names and social security numbers on agency documents. If an agency submits incorrect RTN or address information, the financial institution or the U.S. Postal Service will return a misdirected payment.

b. How will data be checked for completeness? The Legal Administrative Specialists and Program Analysts review the submissions at the time it is received to 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?

Refer to applicable sections of the Application Definition Document for this information.

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? 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—no new data or previously unavailable data will be derived through aggregation from data collected.

3) Will the new data be placed in the individual's record? *Not applicable; system does not derive new data.*

4) Can the system make determinations about employees/public that would not be possible without the new data? *Not applicable; system does not derive new data.*

5) How will the new data be verified for relevance and accuracy? *Not applicable; system does not derive new data.*

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

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?
Not applicable; system does not consolidate processes.

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. Data may be retrieved by means

of a personal identifier, which may include a name or system-assigned number.

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.

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.

C. 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?**

Not applicable; system is not operated in more than one site.

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

FMS plans to submit a records schedule to NARA for approval that would provide for the retention of most data in JFS for seven (7) years. The retention periods of data in this system will be based on a records schedule approved by the National Archives and Records Administration (NARA).

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?**

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. After approval, sensitive paper records are shredded and electronic or magnetic storage media are sanitized in accordance with FMS IT Security Standards.

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?** Not Applicable—public policy is not affected.

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.**
Treasury/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.** The Privacy Act systems of records notice will be amended or revised as appropriate to correspond with the records schedule for the Judgment Fund System.

D. <u>ACCESS TO DATA:</u>

1) **Who will have access to the data in the system?**

Data will be accessible by the JFB staff, by the JFS 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 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?
JFS 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 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?** The JFS application 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 JFS. Active auditing of system and application access and the use of individual UserIDs allow enforcement of individual accountability and traceability of user actions.

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—contractors were not involved in the design and development of JFS nor are they involved in any maintenance of JFS.

6) **Do other systems share data or have access to the data in the system? If yes, explain.** Yes, The FASDAS / Momentum Accounting System interfaces with JFS. JFS transfers payment data to FASDAS / Momentum.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?** The Users of JFS and FASDAS with special emphasis on the systems ISSO share responsibility in protecting the personal data shared between the systems.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?** FPAs that have access to the JFS Authorized website can view data submitted for that agency. Justice is the only agency that can view all submitted data.

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 Manager, Judgment Fund Branch and the JFS ISSO and/or the Alternate ISSO and Judgment Fund Authorized Website System Administrator...