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

**Name of Project:** FASDAS/Momentum®
**Project's Unique ID:** FASDAS

## 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 i**nformation collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment 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 Office of Management and Budget (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?**

The following are some of the functions performed by FASD in conjunction with the core financial system: Provide accounting operations and financial services for Treasury Managed Accounts (TMA) and International Assistance Programs (IAP); bill and collect amounts due from Foreign governments and Federal Agencies; report investment activities of the Foreign Claims Deposit Funds, the Esther Cattell Schmitt Gift Fund, and the Kennedy Center Revenue Bond Sinking Fund; process payments for the Judgment Fund systems (JFS) and the Foreign Claims Programs; make payments to Federal Agencies, the D.C. government, and the public; provide accounting and reporting for the U.S. reserve position in the International Monetary Fund; provide

[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).

accounting and reporting for U.S. contributions to international financial institutions; and process domestic and international letters of credit and draw downs. FASD provides both proprietary and budgetary accounting and reporting for TMA and IAP. FMS provides an accounting service for the Office of the Assistant Secretary for International Affairs, Department of the Treasury, in regard to IAP.

FASDAS/Momentum®, a commercial off-the-shelf core financial system provided by CGI-Federal, performs all of the accounting and budgeting functions related to FASD activities. FASDAS has an interface with the Judgment Fund System. FASDAS replaced GLOWS, the accounting system that was used since the fall of 1998.

FASDAS/Momentum® is compliant with the Joint Financial Management Improvement Program standards.

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

- Chief Financial Officers Act of 1990
- Federal Financial Management Improvement Act of 1996
- OMB Circular A-136
- Government Management Reform Act of 1994
- Government Performance and Results Act of 1993
- Federal Managers' Financial Integrity Act.

## B. DATA in the SYSTEM:

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

The public and State governments

**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?**

Any Federal Agency can submit information.

**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?**

Collected information will be name(s) of claimants as well as the SSN/EIN and addresses or banking information for claimants or persons receiving payments.

**3. Accuracy, Timeliness, and Reliability**

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

The submitting agency certifies to the accuracy of the 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, data elements are described in detail in the functional and data requirements documents.

## 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. Payments could not be made without this information.

**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? Can it be retrieved by personal identifier? If yes, explain. How are the effects to be mitigated?**

   Data may be retrieved by means of a personal identifier such as the vendor code which is usually the payee's last name.

   An authorized user can enter a personal identifier such as the payee's last name to inquire about whether a payment has been made to an individual.

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 can produce reports regarding payments made for a particular individual. Only authorized users have access to these reports.

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 FPA. Such information must be provided if the person wants to receive a payment.

## D. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1. **If the system is in operation at 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?**

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

   The electronic data will be erased and copies of reports will be shredded. The procedures are documented in the FMS information technology security standards and the Manual of Administration.

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.**

   No.

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

   NA

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

   NA

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.*)

   FMS internal users only (i.e., no contractors) there are less than 40 internal users. IR also has access to the platform and servers for maintenance.

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

   FASDAS 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 FASDAS information system security officer (ISSO) or system administrators.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**

   FASDAS users will have restricted access to data. 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 FASDAS ISSO or system administrators.

   Roles have been defined and are used to grant access to each user. Specific roles have been defined for administrators, data entry operators, accountants, and reviewers. Active auditing of system and application access and the use of individual user ids allow enforcement of individual accountability and traceability of user actions.

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*)

FASDAS uses several associated components contained within the general support system (GSS) located at the FMS Hyattsville Regional Operations Center (HROC). GSS components provide both functionality and some security services for FASDAS.

FASDAS users complete access forms and rules of behavior before being granted access to the system. User access will be granted depending on their role in the system. Users are given a unique login identification name and then they are required to set a unique password. Both items are required for login. Audit logs are reviewed weekly to identify any unauthorized login attempts.

Roles have been defined and are used to grant access to each user. Specific roles have been defined for administrators, data entry operators, accountants, and reviewers. Active auditing of system and application access and the use of individual user ids 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?**

   No

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

   Yes, FASDAS has an interface with JFS. Payment information is imported into FASDAS and payment confirmation information is exported into JFS.

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

   The ISSOs

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

   No

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

   NA

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

    The ISSOs