



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 3, 2011

Document Version: Version 2.0

Name of System: Automated Standard Application for Payments (ASAP)

SYSTEM GENERAL INFORMATION:

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

ASAP is an Internet payment mechanism that assists Federal Agencies in disbursing monies to states, municipalities, nonprofit and for profit entities, universities, and financial institutions.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

ASAP's SORN number and type is .016 – Payment Records for Other than Regular Recurring Benefits Payments

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, ASAP contains information about individual members of the public.

b. Is the information about employees or contractors?

No

5) What legal authority authorizes the purchase or development of this system?

By statute, Treasury has the authority to disburse public funds for executive branch agencies, 31 USC 3321. Also, Treasury disbursing officials may only disburse funds in accordance with a payment certification voucher received from a paying agency, 31 USC 3325. ASAP is a disbursement program, which is authorized under these two statutes.

DATA in the SYSTEM:

1) Identify the category of individuals in the system

Check all that apply:

- Employees**
- Contractors**
- Taxpayers**
- Others (describe)** – The individuals are Federal Grant recipients and Program Agencies.

2) Identify the sources of information in the system

Check all that apply:

- Employee**
- Public**
- Federal agencies**
- State and local agencies**
- Third party**

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

None

b. What information will be collected from the public?

Name, address, phone number, and email address.

c. What Federal agencies are providing data for use in the system?

Defense Finance and Accounting Services

Library of Congress

Department of Agriculture

Food and Nutrition Service

Forest Service

National Institute of Food and Agriculture

Department of Commerce

National Institute of Standards and Technology

National Oceanic and Atmospheric Administration

Economic Development Administration

Department of Interior

Bureau of Reclamation

US Geological Survey

National Park Service

Office of Surface Mining

Bureau of Land Management

Minerals Management Service

Naval Sea Systems Command

Department of State

Bureau of Public Debt

Office of Personnel Management

Social Security Administration

Nuclear Regulatory Commission

General Services Administration

Environmental Protection Agency

US Postal Service

Department of Transportation

Department of Homeland Security

Coast Guard

Immigration and Customs

Department of Health and Human Services
Center for Medicare and Medicaid Services
Department of Energy

d. What State and local agencies are providing data for use in the system?

Various offices of all 50 states and territories, including but not limited to:

Department of Employment Services
Department of Natural Resources
Department of Environmental Management
State Comptroller
Health and Mental Hygiene
Job and Family Services
Department of Labor
Division of Unemployment Insurance

e. From what other third party sources will data be collected?

N/A

3) Accuracy, Timeliness, and Reliability

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

Data collected from sources other than FMS is verified for accuracy by the entity which owns the data.

b. How will data be checked for completeness?

ASAP has required fields with edits to ensure completeness of data to the minimum standards specified in requirements documents.

c. What steps or procedures are taken to ensure the data is current?

ASAP users are provided a means to keep their information current through the application online screens, i.e. Modify My Information. It is the sole responsibility of the individual user to maintain his own information, and it is the responsibility of the Authorizing Official to keep the list of users and roles for their organization up to date. Additionally, User IDs are rendered inactive after 90 days of non-use, requiring system administrator assistance to re-activate with current information.

d. In what document(s) are the data elements described in detail?

The data elements are described in detail in the requirements documents for the Modify My Information – RO module of the application.

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 data is relevant and necessary because it serves as a unique identifier for each user and is required for grantees receiving funding from the Federal Government..

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?

ASAP will not derive new data or create previously unavailable data about an individual through aggregation from the collected information.

- 3) **Will the new data be placed in the individual's record?**

N/A

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

N/A

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

N/A

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

ASAP implements and maintains significant and comprehensive security features to ensure that risks, threats, and vulnerabilities are minimized. These are outlined in the System Security Plan.

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

N/A

- 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.)**

Users must enter a password and ID to access their own data in the application and view other users assigned to their organization if their role allows access.

- 9) **What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

A report that allows users to view their own data and data that they have least privilege role based access to. The reports will be used to verify enrollment information and will be used by Recipient Organizations, Federal Agencies, Regional Financial Centers, and the Federal Reserve Bank of Richmond.

- 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?**

ASAP has required and non required fields and individuals may decline to provide any non required information.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

- 1) **What are the retention periods of data in this system? How long will the reports produced be kept?**

Individual information in the system is retained indefinitely, including user accounts that have been suspended. Old information that has been updated by an authorized user is not retained. All transactional data is maintained permanently in ASAP.

- 2) **What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?**

As of November 1999, all ASAP reports have been assigned a retention period of 99 years. This is documented in the FRB/FMS SLA.

- 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?**
 ASAP's database is hosted in the FRIT mainframe environment with redundancy between East Rutherford, NJ and Dallas, TX. All data collected in one site is written to the other. Refer to the system Contingency Plan for maintenance and disaster recovery information.
- 4) **Is the system using technologies in ways that FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
 ASAP is not currently using any technology that FMS has not previously employed.
- 5) **How does the use of this technology affect employee or public privacy?**
 N/A
- 6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
 No
- 7) **What kind of information is collected as a function of the monitoring of individuals?**
 ASAP does not collect data to monitor individuals.
- 8) **What controls will be used to prevent unauthorized monitoring?**
 N/A

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**
 - Others (explain)_____**
 N/A
- 2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**
 Access to data by user is determined by the roles requested when access to the system is granted.
- 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 to their own data once being identified by user name and password. The user will also be restricted through least privileges by role based access.
- 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)**
 User access will be restricted to their own data once being identified by user name and password. The user will also be restricted through least privileges by role based access.
- 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, the MOU between FMS and the FRB Richmond has Privacy Act clauses.
- 6) **Do other systems share data or have access to the data in the system?**
 - yes**
 - no**

If yes,

a. Explain the interface.

Interfaces with Federal Agencies provide detailed payment data and user data is stored in the LDAP.

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

Elizabeth Oldenburg, system owner, is responsible for protecting the privacy rights of the public and employees.

7) Will other agencies share data or have access to the data in this system?

yes

no

If yes,

a. Check all that apply:

Federal

State

Local

Other (explain) _____

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

Federal agencies receive end of day transaction reports for accounting purposes.

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

The Federal Agencies assume responsibility for the data once it is accessed by them.

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