



## ***The Bureau of the Fiscal Service***

### ***Privacy Impact Assessment***

The mission of the Bureau of the Fiscal Service (Fiscal Service) is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

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

Fiscal Service Privacy – Public Debt Impact Assessments  
(PIA): [http://www.treasurydirect.gov/privacy\\_impactassessment.htm](http://www.treasurydirect.gov/privacy_impactassessment.htm)

Document Date: September 15, 2011

Document Version: 3.0.0

Name of System: Integrated Document Management System (IDMS)

**SYSTEM GENERAL INFORMATION:**

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

The Integrated Document Management System (IDMS) has been implemented at BDMOC to archive the various offset checks, letters and warning notices generated by the Treasury Offset Program (TOP) payment process. AFP files generated by TOP are archived in IDMS. Documentation and correspondence associated with FedDebt are archived via this system. Debt and Debtor correspondence associated with DMSC; including TINs, are archived in IDMS. Legislative and Public Affairs will store Debt inquiries, Check inquiries, unclaimed funds, Surety bond issues, Judgment Funds, Direct Deposit issues and Tax Refund offset inquiries

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

.014 Debt Collection Operations System

3) If the system is being modified, will the SORN require amendment or revision?

Yes, explain.

No

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

Yes

No

a. Is the information about members of the public?

Yes

DATA in the SYSTEM:

- 1) Identify the category of individuals in the system

Check all that apply:

Employees

Contractors

Taxpayers

Others (describe) Individuals who have delinquent federal and state debts.

- 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 directly. All information comes from other FMS systems.

- b. What information will be collected from the public?

None directly. All information comes from other FMS systems.

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

Information is input into IDMS by FMS Regional Financial Centers other FMS systems.

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

State agencies are providing data through the TOP system. This data is not received directly.

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

None

The data elements are described in the *IDMS Security Plan*. IDMS maintains data records that consist of Federal and state delinquent debtor's taxpayer identification number (TIN)- which can be either a social security number (SSN) or an employee identification number (EIN), debtor name, address, debtor status, and debt information.

#### 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 in use is both relevant and necessary for the purpose of fulfilling the Debt Collection Improvement Act.

- 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?

No new data or previously unavailable data is created by the IDMS through this aggregation. All data comes from other systems.

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

No new data will be created by the IDMS.

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

No new data will be created by the IDMS.

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

No new data will be created by the IDMS.

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

FMS and IDMS System security protects the data from unauthorized access and use.

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

Reports on individuals can be produced based on taxpayer identification numbers, debt number, name and other criteria. These reports will be used to research information on the case. IDMS users are restricted to only the functions they need for the performance of their duties.

- 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?

Individuals added to IDMS do not have the ability to grant or decline consent to being submitted to IDMS. Documents in IDMS are sent by the creditor agencies participating in Cross-Servicing. In addition, additional information on the individual is sent by TOP, Cross-Servicing and the other FMS processes. Documents within the IDMS are electronically scanned images of original documents. These documents are sent to IDMS on a voluntary basis in response to FMS Debt Collection activities by the various agencies submitting the information.

#### MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

Currently there are no retention guidelines in place. The data is retained indefinitely.

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

Currently there are no retention guidelines in place. The data is retained indefinitely and stored in the IDMS database.

- 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?

FMS maintains consistent use of the system and data at all sites by the development

7) What kind of information is collected as a function of the monitoring of individuals?

Individuals are not monitored in IDMS. However, the Audit Trail report retrieves information on the user id, reference number and the timestamp of the queries performed by the user.

8) What controls will be used to prevent unauthorized monitoring?

N/A. ACC

ESS 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)\_ \_\_\_\_\_

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

All users are restricted to only the functions they need for the performance of their duties. For example, regular users cannot access the system audit logs. User level of access is authorized and reviewed regularly to ensure that user access does not exceed position requirements for all systems and applications. Risk levels are associated with job descriptions to determine access levels for the IDMS application. Managerial approval is required before a user is granted access to functions within the IDMS application.

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

IDMS users are restricted to only the functions they need for the performance of their duties. Only a limited number of individuals associated with TOP have the highest

- 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?

IDMS is a COTS application; however it is maintained by contractors. Privacy Act contract clauses are inserted into their contracts and they are required to take the FMS IT Security training and Disclosure training annually.

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

Yes

No

**If** yes,

- a. Explain the interface.

N/A

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

N/A

- 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.