Financial Management Service
IDMS Privacy Impact Assessment

Name of Project: Integrated Document Management System (IDMS)
Project's Unique ID: IDMS

Once the Privacy Impact Assessment (PIA) is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- FMS IT Security Manager
- FMS AC-area Privacy Act Liaison

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

For purposes of completing any FMS PIA, "data" means any information on an individual in identifiable form, i.e., any information that can be used to identify an individual.

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

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

Yes

c. Is the information about employees?

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).

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

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.

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

The Debt Collection Improvement Act of 1996, Public Law 140-134, April 26, 1996, 110 Stat. 1321 – 1358.

B. DATA in the SYSTEM:

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

Taxpayers and their representatives

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?**

Documents are received from individuals who communicate with FMS regarding debts owed to the United States. Documents are sent to IDMS in response to FMS Debt Collection activities and include: correspondence received from individuals, payment information, offset information.

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

IDMS does not interface with systems outside FMSnet. Information is input into IDMS by KFC, SFC, FedDebt and TOP.

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

IDMS does not interface with systems outside FMSnet.

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

None. IDMS does not interface with systems outside FMSnet.

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

None. IDMS does not interface with systems outside FMSnet.

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

a. **How will data collected from sources other than FMS records be verified for accuracy?**
IDMS does not interface with systems outside FMSnet.

b. **How will data be checked for completeness?**
Not applicable

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).**
Not applicable

d. **Are the data elements described in detail and documented? If yes, what is the name of the document?**
Yes. IDMS Security Plan and IDMS Systems Operations Manual.

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?**
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. IDMS archives and stores data.

3) **Will the new data be placed in the individual's record?**
No

4) **Can the system make determinations about employees/public that would not be possible without the new data?**
No

5) **How will the new data be verified for relevance and accuracy?**
IDMS does not create 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, the data is not being consolidated.

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

Data is not consolidated.

8) **How will the data 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 is retrieved by the documents index value. The index value is determined at the time the document is scanned and indexed. This could be the SSN, individual name, case number, etc.

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.)**

Documents within the IDMS are electronically scanned images of original documents which are stored on an IBM P650 LPAR. These documents are sent to IDMS on a voluntary basis in response to FMS Debt Collection activities.

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?**

IDMS is operated and maintained only at one site.

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

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

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?**

Payment Files – relating to the disbursement of offset notices and partial payments. Transferred to FRC when the data is 7 years old. Destroyed when it's 22 years old.
CS NI-425-91-1-349

Magnetic Tape Files
Destroyed after 2 years of the date of creation
CS NI-425-91-1-394

Hold Check Requests
Destroyed when 3 years and 1 month old
CS NI-425-91-1-418

Accounting Files related to payment/offset processing.
Destroyed 6 years and 3 months after period covered by account
CS NI-425-91-1-1-7 and GRS 6-4.a

Progress Sheets
Microfilm in six months cycles and then destroyed
CS NI-425-91-1-353

SF-1098, Schedule of Cancelled Checks
Destroyed 4 years after end of fiscal year.
CS NI-425-91-1-373

Overpayment and Underpayment Case Files
Destroyed 3 years after end of fiscal year case.
CS NI-425-91-1-360

BDMOC Customer Assistance Files
Tax related Files – 1099C and 1099 Misc forms
After 4 years (Revenue Procedures 97-34, Publication 1220, Part A, General, Section 9, Filing of Information Returns Magnetically/Electronically and Retention Requirements.)

State Offset Reversals – ACH debits through the Federal Reserve Banks.
Destroyed after 4 years.

Treasury Offset Partial Payee Claim Files
Transfer to FRC when 7 years old.
CS NI-425-91-1-349

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?**
   N/A

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?**

N/A

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

N/A

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

Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1998; Treasury / FMS System of Records Notice .014 – Debt Collection Operations System

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

No. N/A

E. ACCESS TO DATA:

1) **Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, other)**

Access to the data has been provided to Users, System Administrators, Contractors and Developers.

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

User access to IDMS is restricted by the operating system security controls, which require a login UserID and password to access the system. User access to system resources is restricted to the minimum necessary to perform the job (i.e., Principle of Least Privilege). Documented in the Security Plan Version 3.2.

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

User access to system resources is restricted to the minimum necessary to perform the job (i.e., Principle of Least Privilege).

Roles	Function Performed
IDMS System Administrator	• Read, Write, and Execute all functions. • Access (root) password(s). • Administer the operating system. • Create/Delete users.

IDMS Database Administrator	• Read, Write, and Execute application data. • Administer database via account. • Access log.
IDMS User	• Read and Execute application data. • Browse access granted data.

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 to IDMS is restricted by the operating system security controls, which require a login UserID and password to access the system. User access to system resources is restricted to the minimum necessary to perform the job (i.e., Principle of Least Privilege). The ISSO and System Administrator provide the user with application access.

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?

Yes. Privacy Act clauses are not included in the IDMS contracts, however, Contractors and Developers are required to take annual Disclosure Training.

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

No

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

N/A

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

IDMS does not interface with systems outside FMSnet.

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

N/A

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

N/A