



## *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: December 15, 2011**

**Document Version: 4.0.0**

**Name of System: Call Tracking System (CTS)**

**SYSTEM GENERAL INFORMATION:**

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

CTS is a interactive database that tracks calls to BDMOC from delinquent debtors inquiring about their delinquent debt.

**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

**b. Is the information about employees or contractors?**

Yes

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

On April 26, 1996, President Clinton signed legislation known as the Debt Collection Improvement Act of 1996 (public Law 104-134). The Debt Collection Improvement Act (DCIA) requires Federal Agencies to refer debts to the Department of the Treasury in order to offset Federal Payments to collect delinquent debts owed to the Federal Government.

**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?**  
Call History and Notes from call
- b. What information will be collected from the public?**  
Call History and TIN for verification of the debt.
- c. What Federal agencies are providing data for use in the system?**  
None directly. All information comes from other FMS systems.
- d. What State and local agencies are providing data for use in the system?**  
None directly. All information comes from other FMS systems.
- e. From what other third party sources will data be collected?**  
None

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

- a. How will data collected from sources, other than FMS records, be verified for accuracy?**  
The information is input by the customer service representative answering the call.
- b. How will data be checked for completeness?**  
The information is input by the customer service representative answering the call.
- c. What steps or procedures are taken to ensure the data is current?**  
CTS is updated when a taxpayer calls into the Call Center to check the status of an offset. Data is selected from an pre-populated list and is selected by the Call Representative during the call.
- d. In what document(s) are the data elements described in detail?**  
The data elements are described in the *CTS Security Plan*. CTS 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, debt information, and call history.

**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?**

Yes, data is collected from the Public calling in to the CTS system.

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

Yes as Call History

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

No.

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

Call history is collected from the Public on a voluntary basis. Callers must identify themselves as the person whose SSN they entered. If it is someone calling on behalf of another person, the actual debtor must be on the line to provide verbal permission for us to speak with the caller or we must have a signed FMS Form 13 or General Power of Attorney already on file before any information is provided. Phone numbers are captured as identifying records for every caller record created in CTS. The fields populated with debtor information are pulled directly from the TOP database. CTS database history records contain the history of the call (Caller telephone number, reason for call, resolution of call, debtor name and TIN). Current Offset and debt (status, reversals, etc.) information is always pulled directly from the TOP database and are not contained in the CTS record created.

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

No data is being consolidated. FMS and CTS System security protects the data from unauthorized access and use

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

No data is being consolidated.

- 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.)**

The debtor provides CTS with a Taxpayer Identification Number (TIN), Employee Identification Number (EIN) or debt number for verification of identity and to retrieve debt and debtor information.

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

The CTS application is designed to allow the agents to print an offset report that contains the same type offset/payment information that was originally provided to the debtor in the offset notice. The agents may also print out individual internal call history reports that contain information like the TIN, time of call, reason for call,

resolution provided, and any special notes entered by the agent receiving the call. These call history reports do not contain any specific offset or debt 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)? How can individuals grant consent?**

Information provided to CTS is strictly voluntary.

### **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 CTS 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?**

No, the systems do not use any new technology that FMS has not previously employed.

- 4) Is the system using technologies in ways that FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No

- 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.**

IDS systems are currently deployed at FMS. In addition to IDS, as a guard against intrusions and other unauthorized activity and for investigating signs of intrusions.

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

Individuals are not monitored in CTS. 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?**

No audit trails are generated in CTS.

### **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) \_\_\_\_\_**

**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 CTS application. Managerial approval is required before a user is granted access to functions within the CTS application.

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

CTS users are restricted to only the functions they need for the performance of their duties. Only a limited number of individuals associated with CTS have the highest level of access. Access rights are reviewed for continuing need at each level.

**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)**

The CTS application management is committed to supporting least privilege and logical access control. CTS application users are restricted to only the functions they need for the performance of their duties. Access rights are reviewed periodically to appropriate levels. In addition, CTS users must consent to the disclosure agreement displayed when logged on before they can proceed to the main menu. CTS users also must sign and submit to the CTS Rules of Behavior to prevent unauthorized monitoring.

**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 this system was designed and developed by contractors. It is also 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.**

CTS does not share information nor do any other systems have access to the data within CTS.

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

The Financial Management Service, Information Owners and System Managers will be responsible for protecting the privacy rights of the individuals affected by the interface.

**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.**

CTS information is not used by other agencies.

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

The Financial Management Service, Information Owners and System Managers will be responsible for protecting the privacy rights of the individuals affected by the interface.