Investigative Scanning & Document Management (ISDM)
Privacy Impact Assessment

PIA Approval Date – July 8, 2008

Requested Operational Date – Feb. 2009

System Overview

ISDM endeavors to create a system that will benefit CI by allowing employees to manage investigations using digital images rather than paper. The solution is flexible where employees can store and transport investigative data while working on a case. Employees will be able to send their imaged and digital documents into case folders where they can be analyzed, reviewed and managed. This improvement enables Special Agents to electronically analyze investigative data by using tools to flag, annotate, redact and highlight these searchable document images. Incorporating the use of OCR text features on all scanned products will allow agents to search thousands of pages of documents through simple keyword searches with improved response time for retrieval.

Systems of Records Notice (SORN):

- **Treas/IRS 34.037**-- IRS Audit Trail and Security Records System
- **Treas/IRS IRS 46.002**--Criminal Investigation Management Information System
- **Treas/IRS 46.003**--Confidential Informants
- **Treas/IRS 46.005**--Electronic Surveillance File
- **Treas/IRS 46.009**--Centralized Evaluation and Processing of Information Items (CEPIIs), Evaluation and Processing of Information (EOI) (formerly: Centralized Evaluation and Processing of Information Items (CEPIIs), Evaluation and Processing of Information (EOI), Criminal Division)
- **Treas/IRS 46.050**--Automated Information Analysis System

DATA IN THE SYSTEM

1. DESCRIBE THE INFORMATION (DATA ELEMENTS AND FIELDS) AVAILABLE IN THE SYSTEM IN THE FOLLOWING CATEGORIES:

TAXPAYER:

ISDM MAY CONTAIN THE FOLLOWING TAXPAYER INFORMATION:

- FIRST AND LAST NAME
- ADDRESS (INCLUDING COUNTRY)
- PHONE NUMBER
- SOCIAL SECURITY NUMBER (SSN) (THE USE OF SSN/TIN DATA IS RELEVANT IN ORDER TO RETRIEVE THE APPROVED FORM FOR LATER REFERENCE, AS NEEDED.)
- TAXPAYER IDENTIFICATION NUMBER (TIN)
- DATES AND STATUS OF CORRESPONDENCE
- CASE STATUS

EMPLOYEE:
ISDM CONTAINS THE FOLLOWING EMPLOYEE INFORMATION:

- INVESTIGATOR ASSIGNED TO THE CASE (USER ID)

AUDIT TRAIL INFORMATION:
ISDM CONTAINS THE FOLLOWING AUDIT TRAIL INFORMATION:

- INVESTIGATOR ASSIGNED TO THE CASE (USER ID)
- TIME AND DATE OF ACCESS

OTHER:
DATA OBTAINED FROM OTHER EVIDENTIARY SOURCES.

2. DESCRIBE/IDENTIFY WHICH DATA ELEMENTS ARE OBTAINED FROM FILES, DATABASES, INDIVIDUALS, OR ANY OTHER SOURCES.

IRS: ISDM DOES NOT OBTAIN ANY DATA ELEMENTS FROM IRS FILES OR DATABASES.

TAXPAYER: THE FOLLOWING DATA ELEMENTS FROM SCANNED DOCUMENTS ARE COLLECTED BY AUTHORIZED CI PERSONNEL:

- SSN/TIN
- NAME OF TAXPAYER
- NAME OF AUTHORIZED REPRESENTATIVE (IF ANY)
- ADDRESS
- PHONE NUMBER
- LEGAL ORGANIZATION NAME
- AUTHORIZED REPRESENTATIVE
- OTHER EVIDENTIARY DATA

EMPLOYEE: THE INVESTIGATOR ASSIGNED TO THE CASE WILL ENTER THE FOLLOWING DATA ELEMENTS:

- USER ID
- STATUS OF CASE
- HISTORY INFORMATION

(NOTE: EACH FILE HAS A HISTORY SECTION WHERE ALL CORRESPONDENCE AND OTHER ACTIONS ARE RECORDED. ONLY AUTHORIZED CI PERSONNEL HAVE ACCESS TO THESE FILES.)

OTHER FEDERAL AGENCIES: NO FEDERAL AGENCIES PROVIDE DATA TO ISDM.

STATE AND LOCAL AGENCIES: NO FEDERAL AGENCIES PROVIDE DATA TO ISDM.

OTHER THIRD PARTY SOURCES: NO FEDERAL AGENCIES PROVIDE DATA TO ISDM.

3. IS EACH DATA ITEM REQUIRED FOR THE BUSINESS PURPOSE OF THE SYSTEM? EXPLAIN.
YES. THE DATA ITEMS IN ISDM ARE USED TO SUPPORT TAX LAW ENFORCEMENT. EACH DATA ITEM IS USED BY APPROPRIATE CRIMINAL INVESTIGATION PERSONNEL IN RESEARCH AND CASE MANAGEMENT.

4. HOW WILL EACH DATA ITEM BE VERIFIED FOR ACCURACY, TIMELINESS, AND COMPLETENESS?
AUTHORIZED CI PERSONNEL REVIEW THE RESULTS OF THE OPTICAL CHARACTER RECOGNITION (OCR) AND SCANNING PROCESS TO DETERMINE ACCURACY, TIMELINESS AND COMPLETENESS. THESE PERSONNEL CAN THEN COMPARE THE ELECTRONIC IMAGE WITH THE SOURCE DOCUMENT.

5. IS THERE ANOTHER SOURCE FOR THE DATA? EXPLAIN HOW THAT SOURCE IS OR IS NOT USED.
NO.

6. GENERALLY, HOW WILL DATA BE RETRIEVED BY THE USER?
DATA RETRIEVAL WITHIN ISDM IS PERMITTED THROUGH APPROVED USE OF THE "QUERY" OR "SEARCH" COMMANDS. AND “FIND” OR “SEARCH” COMMANDS IN THE .PDF. ONLY AUTHORIZED USERS MAY QUERY DATA BY NAME, TIN, STATUS OR AD HOC QUERIES.

7. IS THE DATA RETRIEVABLE BY A PERSONAL IDENTIFIER SUCH AS NAME, SSN, OR OTHER UNIQUE IDENTIFIER?
YES. USERS MAY QUERY DATA BY NAME, TIN OR STATUS.

ACCESS TO THE DATA

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
There are two roles in ISDM, Users and Administrators (system and database): The users are Criminal Investigators in the CI Organization.

Role:
Users
Permissions:

- Add/Update/Read/ Delete data in database as necessary to support law enforcement investigations..
- Print ad hoc reports upon request from approved requestors.

Role:
Repository Administrator
Permissions:

- Add/Update/Read/ Delete repository objects but only as authorized and directed in production transmittals.

Role:
System Administrator
Permissions:

- View, create, update and edit changes to the overall system.
- ISDM SYSTEM ADMINISTRATORS (SAS) ARE RESPONSIBLE FOR ENSURING LAW ENFORCEMENT MANUAL (LEM) SCANS ARE DONE QUARTERLY AND PATCHES ARE UPDATED ON A REGULAR BASIS.

9. HOW IS ACCESS TO THE DATA BY A USER DETERMINED AND BY WHOM?
THE INVESTIGATOR (USER), MANAGER AND SYSTEM ADMINISTRATOR WILL HAVE ACCESS TO DATA IN ISDM BASED ON A NEED-TO-KNOW BASIS. THE USER MUST COMPLETE AN ONLINE FORM 5081, INFORMATION SYSTEM USER REGISTRATION/CHANGE REQUEST, TO REQUEST ACCESS TO THE APPLICATION. THE APPROVAL MANAGER THEN REQUESTS THAT THE USER BE ADDED TO THE ACCESS CONTROL TABLES FOR AN INDIVIDUAL CASE. A USER'S ACCESS TO THE DATA TERMINATES WHEN IT IS NO LONGER REQUIRED. CRITERIA, PROCEDURES, CONTROLS, AND RESPONSIBILITIES REGARDING ACCESS ARE DOCUMENTED IN THE INFORMATION SYSTEMS SECURITY RULES.

THERE IS NO CONTRACTOR ACCESS TO ISDM.

10. DO OTHER IRS SYSTEMS PROVIDE, RECEIVE, OR SHARE DATA IN THE SYSTEM? IF YES, LIST THE SYSTEM(S) AND DESCRIBE WHICH DATA IS SHARED.
NO. OTHER IRS SYSTEMS DO NOT PROVIDE, RECEIVE, OR SHARE DATA ELECTRONICALLY WITHIN THE SYSTEM.

11. HAVE THE IRS SYSTEMS DESCRIBED IN ITEM 10 RECEIVED AN APPROVED SECURITY CERTIFICATION AND PRIVACY IMPACT ASSESSMENT?
NOT APPLICABLE.

12. WILL OTHER AGENCIES PROVIDE, RECEIVE, OR SHARE DATA IN ANY FORM WITH THIS SYSTEM?
NO. OTHER AGENCIES DO NOT PROVIDE, RECEIVE, OR SHARE DATA IN ANY FORM WITH THIS SYSTEM.

ADMINISTRATIVE CONTROLS OF DATA

13. What are the procedures for eliminating the data at the end of the retention period?
Procedures for eliminating data after the retention period are performed in accordance with Internal Revenue Manual (IRM) 1.15.30-1 item number 15, Investigative Files - Records Management, Records Control Schedule for Criminal Investigation, January 1, 2003.

The retention period does not begin until the case or investigation is closed. At the end of the 2 year retention period the data will be removed from the database via a scheduled maintenance task.

14. Will this system use technology in a new way?
No. This system will not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups?
Yes. ISDM is used to store information related to ongoing cases. Information related to these individuals may be used to identify or locate individuals or groups associated with the investigation.

16. Will this system provide the capability to monitor individuals or groups?
Yes. ISDM is used to store information related to ongoing cases. Information related to these individuals may be used to monitor individuals or groups associated with the investigation. Only authorized CI personnel may access individual assigned case files.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. There is no disparate treatment of employees or taxpayers. ISDM automates a paper process and consolidates information from taxpayers into a database.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
The ISDM has no part in ensuring due process. It is solely a document repository..

19. If the system is Web-based, does it use persistent cookies or other tracking devices to identify Web visitors?
ISDM is a Web-based application but does not use persistent cookies or other tracking devices. In addition, it is an intranet application with no public Web visitors having access to the system.

View other PIAs on IRS.gov