Issue Management System (IMS) Release 3.6 – Privacy Impact Assessment

PIA Approval Date – Mar. 8, 2011

System Overview:

To better manage the audit process, Large Business and International (LB&I) developed an application, Issue Management System (IMS) Release 3.6. IMS Release 3.6 provides LB&I with an automated tool to assist its examiners and examination teams in the examination process. IMS Release 3.6 provides an issue–driven compliance approach, which identifies and investigates issues. The application collects issue–based information on audits in a way that makes it available centrally for exam monitoring and strategy development. The data that is collected is used by the Issue Based Management System (IBMIS) for reporting purposes. The IMS Release 3.5 application modification was recently upgraded to IMS Release 3.6 into an Enterprise Architecture compliant application. In addition, many of LB&I's functionalities such as Tax Treaty, Audit, Exchange of Information, etc. was integrated into IMS Release 3.6 to minimize the duplication of data and to provide a centralized interface for all related compliance review activities. These improvements allow agents to be more effective, increase their performance, and provide better customer service.

Systems of Records Notice (SORN):

- IRS 34.037--Audit Trail and Security Records
- IRS 42.001--Examination Administrative File
- IRS 42.002--Excise Compliance Programs
- IRS 42.008--Audit Information Management System (AIMS)

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer – IMS contains corporate and estate taxpayer data, which automatically creates IMS cases consisting of one or more tax returns for the same taxpaying entity. Corporate data from ERCS (Examination Returns Control System) is the primary source for the IMS Repository. Tables are created, which represent each of the following tax forms: 720, 720–TO, 720–CS, 2290, 730, 706, 709, 11–C, 637, 8849, 941, 1042, 1065, and 1120. Types of data collected include:
   - Taxpayer Identification Number (TIN)
   - Taxpayer Business ID
   - Business Name
   - Taxpayer Contact Name
   - Professional Title
   - Tax Return Exam ID and Filing Period
   - Address
   - Relationship
   - Telephone Number
   - Percent of Stock Ownership by Corporate Officer

B. Employee – IMS collects information on the employee working on the taxpayer account. Types of information collected include:
   - IRS Employee Name
   - Time Worked (provides manager information needed to track and report statistics, including time spent working an issue, who is working an issue, and who is available for issue assignment)

- Position (user class for security level)
- User ID

C. Audit Trail Information – IMS has application audit logging configured in accordance with Internal Revenue Manual (IRM) 10.8.3. The application audits events involving case creation, adding entities, issues, and team members on a case. The audit function collects the following data:

- Time Worked on Issue
- Update Timestamp
- Entry Timestamp
- User ID/entry User ID
- Password

IMS integration provides a single entry timekeeping function for each examiner. Using time tracked by issue, IMS provides the following reports for each examiner, which are automatically populated from the one time entry:

- Prepare the Form 3081 for Payroll
- Prepare the ERCS Time Input Report for Updating Summary Examination Time Transmission System (SETTS)
- Prepare the Form 9984 (Examining Officer's Activity Record)
- Reports for Management Accounting for Non–Direct Examination Time

D. Other – Other data elements and fields within the IMS application include several conceptual entity categories such as:

- Tax Returns 720, 720–TO, 720–CS, 2290, 730, 706, 709, 11–C, 637, 8849, 941, 1042, 1065, and 1120 and data in forms
- Cases
- Case Information
- Case Resolution
- Work Items
- Work Item Comments
- Work Item Communications
- Work Item Information
- Work Item Issue
- Work Item Notice
- Work Item Status
- Issue
- SAIN (Standard Accounting Index Number)
- Uniform Issue Listing
- Major SAINs (Standard Accounting Index Numbers) include:

SAIN #	Title
100's	Asset Accounts
200's	Liability Accounts
300's	Capital Accounts
400's	Income Accounts
500's	Expense Accounts
600's	Special Deductions and Credits
700's	General Information
Misc.	Miscellaneous

The following are SAIN categories:

- EX014 – Aviation Fuel – Gas
- EX016 – Petroleum – Imported
- EX017 – Imported Chemical
- EX018 – Oil Spill – Domestic
- EX019 – ODC
- EX020 – FLR. STK. ODC
- EX021 – Oil Spill – Imported
- EX022 –Telephone
- EX026 – Trans Of Persons By Air
- EX027 – Use INT'ALl Air Facilities
- EX028 – Trans Of Property By Air
- EX029 – Trans Persons By Water
- EX030 – Foreign Insurers
- EX031 – Obligations Not In Reg
- EX032 – Pistols & Revolvers
- EX033 – Trucks Retail
- EX034 – Structured Settlement
- EX035 – Kerosene Tax
- EX036 – Coal – Underground Mined
- EX037 – Coal – Underground % Of Sales Price
- EX038 – Coal – Surface Mined
- EX039 – Coal – Surface Mined % Of Sales Price
- EX040 – Gas Guzzler
- EX041 – Fishing Equipment
- EX042 –Trolling, Sonar
- EX044 – Bows, Quivers, Broadheads, And Points
- EX046 – Firearms (Not # 32)
- EX049 – Shells & Cartridges
- EX050 – WPT
- EX051- Alcohol Not Used As Fuel
- EX052- WPT – Annual
- EX053- Petroleum – Domestic
- EX054- Chemicals
- EX056- WPT – Withheld
- EX057- FLR. STK. – Tires
- EX058- Gas Sold To Make Gasohol
- EX059 – Gasohol
- EX060 – Diesel

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS – Excise Tax Registration Authentication System (EXTRAS), component of the Excise Files Information Reporting System (ExFIRS) application:

- IMS receives 637 Registration data from the ExFIRS System.

Bureau of National Affairs (BNA) – Corporate Tax Analyzer (CTA) – IMS receives various pieces of data from BNA–CTA, an IRS COTS product including:

- Calculated Adjustments
- Taxable Income per Return
- Taxable Income per Exam
- Payment Indicator
- Disposal Code
- Total Tax per Return
- Total Tax per Exam

Corporate Authoritative Directory Services (CADS) (Part of MITS–17 GSS) – CADS provides employee data feeds to the IMS application including:

- Name of IRS Employee
- Position (user class for security level)
- User ID

Examination Returns Control System (ERCS) – IMS receives return data from ERCS including:

- Taxpayer Identification Number (TIN)
- Taxpayer Business ID
- Business Name
- Taxpayer Contact Name
- Professional Title
- Tax Return Exam ID and Filing Period
- Address
- Relationship
- Telephone Number
- Percent of Stock Ownership by Corporate Officer

B. Taxpayer – The IMS application does not receive information from taxpayers directly.

C. Employee – The IMS application does not receive any information from employees directly except for SEID and Password for login.

3. Is each data item required for the business purpose of the system? Explain.
Yes. Each data item is required for the business purpose of IMS. IMS helps to ensure compliance with tax laws. It also addresses other strategic goals, such as the identification of abusive tax shelters. IMS provides the ability for LB&I staff to share knowledge regarding issues under development, pre-filing agreements, and abusive tax shelters. It also provides a system for issue identification, tracking, and reporting to greatly improve the examination process.

IMS supports two categories:

The tax examination process includes all processes performed to provide tax return and tax case information to revenue agents and processes in support of the actual tax examination.
For tactical and strategic management and planning, IMS gathers key data to enable managers to monitor and control the execution of the examination plan. Issue data gathered across cases and industries provides managers and strategic planners with information regarding trends in tax compliance.

4. How will each data item be verified for accuracy, timeliness, and completeness?
IMS checks for valid data types on screen level to ensure that the correct data is entered into the data fields and does not cause system exceptions. IMS business rules are in place to ensure that only acceptable values are entered and users are restricted from inputting invalid characters in IMS fields. A data link handled by common functions, reads the database and only allows users to enter a set amount of characters (or less; limited input) in any text box based on the database. The application also has SQL injection functions in place to check character sequences restricting users from sending SQL statements to the database for execution. The IMS application checks the validity of source information from other applications as well.

5. Is there another source for the data? Explain how that source is or is not used.
No. There are no other sources for the data in IMS.

6. Generally, how will data be retrieved by the user?
The data can be retrieved by TIN and geographic location of the taxpayer (through ERCS) to an entity under examination, depending on user access permissions.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. The TIN is used for retrieval of data. The team coordinator or manager will assign agents to specific tasks. The User ID assigned to agents will determine the taxpayer data that the user is permitted to access along with the type of access (read, update, delete). All information related to User ID assignment is stored in the User ID entity.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
The table below lists the different user roles that have access to the IMS application and their permission levels. No contractors outside of the IRS have access to the data in the system. All users access the application through the IRS intranet.

Role: System Administrator
Permission: The system administrator has minimal system access, limited to certain configuration and maintenance functions on the web portal.

Role: Primary Team Coordinator (case)
Permission: The primary team coordinator is the creator of a given case and has the highest level of permissions on a given case.

Role: Team Manager (case)
Permission: The team manager assigned to a given case can differ from the direct manager of the PTC on the case. The TM has elevated permissions on the case.

Role: Team Coordinator (case)
Permission: The team coordinator role has permissions in between the PTC/TM and the EC on a given case.

Role: Entity Coordinator (case)
Permission: The entity coordinator has permissions and control over a specific entity on a given case.

Role: Team Member (case)
Permission: The team member role has the lowest level of permissions on a given case.

Role: National Office (org)
Permission: National office is the highest executive management level. A national office user has the widest breadth of access within their respective BOD. This user has access to application case data within the given BOD. It is important to note that national office and BOD are the same level of permissions in IMS.

Role: Industry Manager (org)
Permission: Each BOD is comprised of one or more industries. The industry level user has access to application case data within the given industry.

Role: DFO Manager (org)
Permission: Each industry is comprised of one or more DFOs. The DFO level user has access to application case data with the given DFO.

Role: Territory Manager (org)
Permission: Each DFO is comprised of one or more territories. The territory level user has access to application case data within the given territory.

Role: Team Manager (org)
Permission: Each territory is comprised of one or more teams. The team level user has access to application case data within the given team.

Role: TCN Administrator
Permission: The TCN administrator is the only role with add, edit, and delete capability in the TCN (terminal control number) module on the web portal.

9. How is access to the data by a user determined and by whom?
Case Management will associate the tax return with developing issues, working papers and other data relevant to an audit. The team coordinator or manager will assign individuals or teams needed to complete specific tasks for the examination. Access is granted through the Online 5081 application by the user's manager and the IMS system administrator.

10. Do other IRS systems provide, receive, or share data in the system?
Yes. IMS receives and shares data with other IRS applications including:

- EXTRAS component of the ExFIRS application:
  - IMS receives 637 Registration data from the ExFIRS system.

- Bureau of National Affairs (BNA) – Corporate Tax Analyzer (CTA), an IRS COTS product – IMS receives various pieces of data from BNA–CTA including:
  - Calculated Adjustments
  - Taxable Income per Return
  - Taxable Income per Exam
  - Payment Indicator
  - Disposal Code
  - Total Tax per Return
  - Total Tax per Exam

- Corporate Authoritative Directory Services (CADS) (Part of Modernization and Information Technology Service (MITS)–17 General Support System (GSS)) – CADS provides employee data feeds to the IMS application including:
    - Name of IRS Employee
    - Position (user class for security level)
    - User ID

- Examination Operational Automation Database (EOAD) – IMS sends a flat file containing closed case data to EOAD.

- Examination Returns Control System (ERCS) – IMS receives return data from ERCS including:
    - Taxpayer Identification Number (TIN)
    - Taxpayer Business ID
    - Business Name
    - Taxpayer Contact Name
    - Professional Title
    - Tax Return Exam ID and Filing Period
    - Address
    - Relationship
    - Telephone Number
    - Percent of Stock Ownership by Corporate Officer

- Issue Based Management Information System – Reporting (IBMIS Reporting):
    - IMS provides reporting data to IBMIS.

- Security Audit Analysis System (SAAS) – IMS provides audit data to the SAAS application including:
    - Time Worked on Issue
    - Update Timestamp
    - Entry Timestamp
    - User ID/entry User ID
    - User's Password

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Yes, the IRS systems in Item 10 have received an approved Security Certification and Privacy Impact Assessment except for those systems identified as FISMA non–reportable applications.

Excise Files Information Reporting System (ExFIRS)

- Certification and Accreditation (C&A) Authority to Operate (ATO) – June 26, 2008, expires on June 26, 2011.
- Privacy Impact Assessment (PIA) – March 23, 2009, expires on March 23, 2012.

Bureau of National Affairs (BNA) – Corporate Tax Analyzer (CTA)

- BNA–CTA is not a FISMA reportable application. Therefore, it does not have an approved Security Certification and Privacy Impact Assessment.

Corporate Authoritative Directory Services (CADS) (Part of Modernization and Information Technology Service (MITS)–17General Support System (GSS))

- Certification and Accreditation (C&A) Authority to Operate (ATO) – September 24, 2010, expires on September 24, 2013.
- Privacy Impact Assessment (PIA) – February 19, 2010, expires on February 19, 2013.

Examination Operational Automation Database (EOAD)

- EOAD is not a FISMA reportable application. Therefore, it does not have an approved Security Certification and Privacy Impact Assessment.

Examination Returns Control System (ERCS):

- Certification and Accreditation (C&A) Authority to Operate (ATO) – June 13, 2008, expires on June 13, 2011.
- Privacy Impact Assessment (PIA) – received on March 3, 2008, expires on March 3, 2011.

Issue Based Management Information System – Reporting (IBMIS Reporting)

- Certification and Accreditation (C&A) Authority to Operate (ATO) – June 10, 2008, expires on June 10, 2011.
- Privacy Impact Assessment (PIA) – received on May 20, 2008, expires on May 20, 2011.

Security Audit Analysis System (SAAS)

- Certification and Accreditation (C&A) Authority to Operate (ATO) – June 9, 2008, expires on June 9, 2011.
- Privacy Impact Assessment (PIA) – received on April 9, 2010 expires on April 9, 2013.

12. Will other agencies provide, receive, or share data in any form with this system?
Yes, IMS makes data available to TIGTA as necessary to aid in an investigation. IMS does not provide/receive/share data with any other agencies.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
IMS data is approved for destruction five fiscal years after import to the central repository in accordance with IRM/Records Control Schedule 26 for Tax Administration – International (LB&I), Item 47 (Job No. N1–58–09–105). That National Archives–approved job number also provides (temporary) dispositions for IMS inputs, outputs and system documentation.

14. Will this system use technology in a new way?
No. The system does not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes. IMS uses examination issues to locate groups of non-compliant taxpayers with the tax code. By tracking these issues, the IMS application ensures that the IRS will be in a better position to offer taxpayer assistance to correct or eliminate areas of non–compliance.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
No, the IMS application does not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No, the IMS application does not allow the IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes, all taxpayer rights are the same using the IMS system as an examination is conducted without the use of IMS.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
No, the IMS application does not use persistent cookies or other tracking devices to identify web visitors. Access to the web portal is performed by checking user credentials via Active Directory.

View other PIAs on IRS.gov