Integrated Data Retrieval System (IDRS) – Privacy Impact Assessment

PIA Approval Date – Jul. 12, 2011

System Overview

The Integrated Data Retrieval System (IDRS) is a mission critical system consisting of databases and operating programs that support IRS employees working active tax cases within each business function across the entire IRS. This system manages data that has been retrieved from the Tax Master Files allowing IRS employees to take specific actions on taxpayer account issues, track status and post transaction updates back to the Master Files. Actions taken via IDRS include notice issuance, installment agreement processing, offers in compromise, adjustment processing, penalty and interest computations and explanations, credit and debit transfers within an account or other related accounts and research of taxpayer accounts for problem resolution of taxpayer inquiries. These updates are done in both a batch process and through online interactive real-time programs commonly known in the IRS as Command Codes. IDRS provides for systemic review of case status and notice issuance based on case criteria, alleviating staffing needs and providing consistency in case control.

Systems of Records Notice (SORN):

None. Because IDRS is not a System of Records (SOR), there is no IDRS–specific System of Records Notice or System of Records Number. Therefore, a SORN has not been published in the Federal Register for IDRS. Pursuant to 5 U.S.C. § 552a (a) (5) which defines a System of Records, IDRS is not a System of Records. This is because although IDRS is an access or computer application, or infrastructure or interface, IDRS is not a System of Records as defined by the Privacy Act. This determination was made with the assistance of IRS' Governmental Liaison and Disclosure Office (4/6/2005 and 12/10/2007) and was confirmed by the Treasury Privacy Act Officer in January 2008.

Although there is no IDRS–specific SOR for the reasons indicated above, the applicable SORNs are the following:

- IRS 22.060--Automated Non–Master File
- IRS 24.030--Customer Account Data Engine Individual Master File
- IRS 24.046--Customer Account Data Engine Business Master File
- IRS 34.037--IRS Audit Trail and Security Records System

Data in the System

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

A. Taxpayer – The entity data consists of the taxpayer's:
- SSN
- Address
- Name Control (first four characters of the taxpayer's last name)

The tax module data consists of individual taxpayer data to include the taxpayer's:
- Name
- SSN
- Date of birth
- Address

- Filing status
- Exemptions
- Income, etc.

The business taxpayer data consists of:

- Corporation or partnership name
- Taxpayer Identification Number (TIN)
- Business income, etc.

B. Employee – Information collected consists of:

- Employees' IDRS user–id and password
- IDRS employee number.

C. Audit Trails – Audit trails consist of:

- 10 digit assigned unique employee number
- 10 digit case number
- Tax period.

For example, 0611 (indicates a return filed in June of 2011). These fields are entered after the employees have entered their user–id and password. Managers receive a computerized listing that indicates what employee is working on what case(s) and this listing would indicate if an employee was reviewing a taxpayer's information that they had not be assigned. There are other computerized programs that provide both audit trails and statistics as to whether an employee made an unauthorized access (UNAX) of a taxpayer's tax data.

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

A. IRS – Taxpayer Information File (TIF); Integrated Data Retrieval System consists of 90 TIF Records. These 90 TIF records vary by type/functionality and depending upon their type are used by the Small Business/Self Employed (SB/SE) Operating Division, Large Business & International (LB&I) Operating Division, Tax Exempt and Government Entities (TE/GE) Operating Division and Wage & Investment (W&I) Operating Division, and Appeals.

B. Taxpayer – The IDRS contains taxpayer data information provided by taxpayers via the information they provided in their tax returns and includes:

- Entity data
- Tax Module data
- IDRS data.

C. Employee – Information is collected from employees who are authorized to log on and work and process requests such as audits, payment and collection activities. This information is tracked via audit trails on the Online 5081 (OL5081) system; audit trails contain the employee's number which is used by IDRS to assign tax cases to a particular employee.

D. Other Federal Agencies:

- The Department of the Treasury's Financial Management System (FMS) sends the IRS a file known as the "Disposition" file that is fed into the Case Control Activity (CCA) process of IDRS.
- Lockbox Processing Systems (Lockbox) supplies payment data to the Taxpayer Delinquent Account (TDA) subsystem of IDRS.

- The United States Postal Service (USPS) supplies data to the TDA subsystem of IDRS.
- The Defense Manpower Data Center (DMDC) supplies data to the TDA subsystem of IDRS.
- The U.S. Department of Agriculture's Federal Payroll Office (FPO) supplies data to the TDA subsystem of IDRS.
- Financial Institutions/Banks send and receive installment agreement payment information to/from the EFT subsystem of IDRS.
- The Government Sponsored Enterprise (GSE), Federal National Mortgage Association (FNMA) sends EIN assignments into the ERAS subsystem of IDRS.

E. State and Local Agencies:
- State and local Governments send data to the State Income Tax Levy Program (SITLP) subsystem of IDRS.
- The Employment Commission Data Exchange (ECDE) supplies data to the TDA subsystem of IDRS.

F. Other Third Party Sources
- Tax professionals submit data to the Reporting Agent File (RAF) subsystem of IDRS.

Note: All files received from outside of IRS are received via underlying Generalized Support Systems (GSSs).

3. Is each data item required for the business purpose of the system? Explain.
Yes. The IDRS allows the designated end-users/employees of the Small Business/Self Employed (SB/SE) Operating Division, Large Business and International (LB&I) Operating Division, Tax Exempt and Government Entities (TE/GE) Operating Division, Wage & Investment (W&I) Operating Division, and Appeals within the IRS who have been assigned a caseload related to their specific function (examination, audit, collection, etc.) to access the data they need to conduct review of requests for their respective functions from the IDRS.

4. How will each data item be verified for accuracy, timeliness, and completeness?
The various programs and command codes within the IDRS have built in validity checks to help ensure accuracy. For example, there are validity checks to insure that a SSN/TIN (when entered into an on-line application) contains all numeric data. Validity checks also are in place (using the previously mentioned entity data) to ensure that if multiple taxpayers have the same first and last name, they are properly distinguished from one another via the entity check information. Product Assurance reviews the data as part of the case processing procedures to aid in ensuring accuracy, timeliness and completeness. There are a series of tests performed on this data such as the Compatibility Test and Final Integration Test which ensures the accuracy, timeliness and completeness of all IDRS data prior to its implementation during the annual Filing Season Start-up.

5. Is there another source for the data? Explain how that source is or is not used.
Yes, some data elements are available from other systems. Those systems are unique to a particular office function, i.e. Appeals, ACS, or Field collection, and are not readily accessible to other office functions. In addition, these systems are not specific to the IDRS cases. The IDRS is specific to maintaining taxpayer information on the Individual Masterfile (IMF), and the Business Masterfile (BMF). Cases are assigned to IRS employees for activities for each Masterfile (i.e. collection, examination, customer service, taxpayer notification etc.).

6. Generally, how will data be retrieved by the user?
Data is retrieved and displayed using command codes on standard IDRS screens.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Data is retrievable by Taxpayer Identification Number (TIN), Document Locator Number (DLN), and collectively the Masterfile Transaction Code and Tax Period.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Only authorized employees (users, managers, database administrators, system administrators, system acceptability testers and final integration testers, developers) in each business unit who as a part of their duties need access. In addition, in the course of their investigative and audit responsibilities, as authorized by the IRS Office of Disclosure, the Treasury Inspector General for Tax Administration (TIGTA) and GAO, may be authorized to receive data from IDRS.

Contractors are authorized to hold the Developer, System Acceptability Testers, and Final Integration Testers roles. Contractors have staff-like access and are authorized by IRS management to perform limited testing and problem resolution, as deemed by their role.

9. How is access to the data by a user determined and by whom?
Management determines which employees have access to the IDRS and for what purposes. The Online 5081 (OL5081) documents at what levels they may view and use the data as a result of each employee who uses IDRS having a profile that determines this level of access. Employee access is determined by their specific need to access taxpayer data to perform their assigned duties. The OL5081 is signed by the employee and the employee's manager. By signing this document each user and their manager would be accountable for their misuse of the system.

Audit trails are produced by the Security and Communications System (SACS). All users must pass through SACS to get access to IDRS.

All contractors are required to comply with the IRS standards for Background Investigation.

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.
Yes. The following IRS systems provide, receive, or share data with IDRS:

- Account Management Services (AMS)
- Adoption Taxpayer Identification Number (ATIN)
- Audit Information Management System Reference (AIMS–R)
- Automated 6020(b) Substitute for Returns (A6020b)
- Automated Collection System (ACS)
- Automated Liens System (ALS)
- Automated Non Master File (ANMF)
- Automated Offers In Compromise (AOIC)
- Automated Substitute for Return (ASFR)
- Automated Trust Fund Recovery Program (ATFR)
- Automated Under Reporter (AUR)
- Branded Prescription Drugs (BPD)
- Business Master File (BMF)
- Corporate Files Online (CFOL)
- Custodial Detail Database (CDDB)

- Electronic Federal Payment Posting System (EFPPS)
- Employee Plans Master File (EPMF)
- Error Resolution System (ERS)
- Federal Tax Deposit System (FTD)
- Generalized IDRS Interface (GII)
- Generalized Mainline Framework (GMF)
- Generalized Unpostable Framework (GUF)
- Individual Master File (IMF)
- Individual Taxpayer Identification Number Real–Time System (ITIN RTS)
- Integrated Collection System (ICS)
- Integrated Customer Communication Environment (ICCE)
- Inventory Delivery System (IDS)
- Microfilm Replacement System (MRS)
- Modernized E–File (MeF)
- Name Search Facility (NSF)
- National Account Profile (NAP)
- Remittance Processing System Pre-mainline (RPS–PM)
- Report Generation Software (RGS)
- Service Center Control File Processing (SCCF)
- Standardized IDRS Access (SIA) – Tier II

These processes send or receive data via files or IDRS command codes. These data exchanges are controlled by the general support systems (GSSs) and all input is protected by access control list which only allows authorized/trusted applications to provide input.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Yes. System owner(s) are responsible for assuring their systems and database are in compliance with all IRS and Government wide mandates, laws, and requirements including Security Certifications and Accreditations, and a Privacy Impact Assessment approval.

12. Will other agencies provide, receive, or share data in any form with this system?
Yes. In the course of their investigative and audit responsibilities, as authorized by the IRS Office of Disclosure, the Treasury Inspector General for Tax Administration (TIGTA) and GAO may be authorized to receive data from IDRS.

- The Department of the Treasury's Financial Management System (FMS) sends the IRS a file known as the “Disposition” file that is fed into the Case Control Activity (CCA) process of IDRS; receives IDRS refunds and check claims from the End of Day (EOD) sub–system of IDRS; and receives Refund Intercepts from the Refunds Intercept Request (RIR, NOR) subsystem of IDRS.
- The Social Security Administration (SSA) receives SS4 forms from the EIN Research and Assignment (ERAS) subsystem of IDRS.
- Financial Institutions/Banks send and receive installment agreement payment information to/from the EFT subsystem of IDRS.
- Lockbox Processing Systems (Lockbox) supplies payment data to the Taxpayer Delinquent Account (TDA) subsystem of IDRS.
- The United States Postal Service (USPS) supplies data to the TDA subsystem of IDRS.
- The Defense Manpower Data Center (DMDC) supplies data to the TDA subsystem of IDRS.
- The U.S. Department of Agriculture's Federal Payroll Office (FPO) supplies data to the TDA subsystem of IDRS.

- The Government Sponsored Enterprise (GSE) Federal National Mortgage Association (FNMA) sends EIN assignments into the ERAS subsystem of IDRS.
- State and local Governments send data to the State Income Tax Levy Program (SITLP) subsystem of IDRS.
- The Employment Commission Data Exchange (ECDE) supplies data to the TDA subsystem of IDRS.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
IDRS does not create, store, and/or manage records as defined under the Federal Records Act (44. U.S.C). Consequently, IDRS does not need to be scheduled as required by 36 CFR, Chapter XII. Any data within the system itself is considered duplicative of data derived from other systems. This determination was made with the assistance of IRS' Office of Records and Information Management (6/24/2011). The data which is passed through by IDRS is not archived and IDRS itself does not maintain a data log or audit information. Systems that interact with IDRS are scheduled as required, or are being scheduled as systems come on–line. The IRS Records Management Office works with IRS Business Owners to obtain the required records dispositions when required.

14. Will this system use technology in a new way?
No. IDRS 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. The records accessed by IDRS contain data that allow designated and authorized IRS employees who have a business need to identify and/or locate individuals or groups. For example, in an instance where a taxpayer applies for and is granted Innocent Spouse Relief the data gleaned from a case where a couple filed their income tax return jointly would then be used to identify and locate the other spouse who is obligated to make the tax payment. Collection activities also use this data to identify and locate taxpayers who have an outstanding tax obligation. Examination also uses this data to identify and locate taxpayers for audit purposes. Appeals uses this data to identify and locate taxpayers who are contesting their tax obligation in U.S. Tax Court.

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.
Yes. The system tracks the status of a taxpayer's account after it has been assigned as a case for audit, collection, appeal, etc. It is intended to identify and locate individuals or groups. Audit trails exist that determine whether or not an IRS employee is authorized to have access and use of the system. These audit trails are determined by assigned employee numbers, user–ids and passwords.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
Yes, use of the system can allow the IRS to treat taxpayers, employees, or others, differently. However, procedures are in place for taxpayers that allow them to have appeal rights for taxes unjustly levied against them. In addition, taxpayers may pursue any tax problems stemming from the misuse of, or unauthorized access of, their tax data by seeking resolution via the Taxpayers Advocate's office. Employees may be treated differently; however, procedures exist that provide protections for the employee so they might not be subject to any unwarranted disciplinary actions. Form 10420, Security Incident Report, and Form 11377, Taxpayer Data Access, provide protections for those IRS employees who accessed a taxpayer's data which had not been assigned to them as a result of a keying error, or inadvertent access.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. The effects of the IDRS on the due process rights of taxpayers are positive and do not need to be mitigated.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
Not applicable. IDRS is an internal application that is not internet–accessible.

View other PIAs on IRS.gov