NOTE: The following reflects the information entered in the PIAMS Website.

A. SYSTEM DESCRIPTION


Date of Approval: 07/18/2014 PIA ID Number: 1001

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):
   Integrated Data Retrieval System, IDRS

2a. Has the name of the system changed? No

   If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

   Number of Employees: _______________________
   Number of Contractors: _______________________
   Members of the Public: Over 1,000,000

4. Responsible Parties:
   NA

5. General Business Purpose of System

   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. Due process is provided pursuant to 26 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (If you do not know, please contact *Privacy and request a search) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 07/12/2011

6b. If Yes, please indicate which of the following changes occurred to require this update.

   • System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) Yes
   • System is undergoing Security Assessment and Authorization Yes

6c. State any changes that have occurred to the system since the last PIA

   None; PIA expires this month (July)

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. 015-000000018

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes
8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

<table>
<thead>
<tr>
<th>Source Type</th>
<th>Taxpayers/Public/Tax Systems</th>
<th>Employees/Personnel/HR Systems</th>
<th>Other Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

<table>
<thead>
<tr>
<th>Type of PII</th>
<th>Collected?</th>
<th>On Public?</th>
<th>On IRS Employees or Contractors?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Social Security Number (SSN)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Tax Payer ID Number (TIN)</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Address</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Additional Types of PII: No

No Other PII Records found.

10a. Briefly describe the PII available in the system referred to in question 10 above.

 Taxpayer – The entity data consists of the Taxpayer’s: SSN Address Name Control (first four characters of the Taxpayer’s last name) Phone numbers Filing status The Tax Module Data consists of individual Taxpayer Data to include the Taxpayer’s: Exemptions Income, etc. The business Taxpayer Data consists of: Corporation or partnership name Taxpayer Identification Number (TIN) Business Income, etc.

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)


10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

None has been identified as yet. When a unified solution is identified to be used by the master files, and interfacing collection systems such as ACS and ICS, it will need to be implemented consistently between all of the interfacing systems.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

N/A
11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is not needed.

Audit Trails consist of: 10 digit assigned unique employee number 10 digit case number Tax period. For example, tax period 200611 (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.

11a. Does the Audit Trail contain the Audit Trail elements as required in current IRM 10.8.3 Audit Logging Security Standards? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:
   a. IRS files and databases: Yes
      If Yes, the system(s) are listed below:
      | System Name                    | Current PIA? | PIA Approval Date | SA & A? | Authorization Date |
      |--------------------------------|--------------|-------------------|---------|--------------------|
      | Taxpayer Information File (TIF)| No           | No                | No      |                    |
      | Integrated Data Retrieval System| Yes         | 07/12/2011        | Yes     | 12/09/2011         |

   b. Other federal agency or agencies: Yes
      If Yes, please list the agency (or agencies) below:
      • 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.
      • 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.

   c. State and local agency or agencies: Yes
      If Yes, please list the agency (or agencies) below:
      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.

   d. Third party sources: Yes
      If yes, the third party sources that were used are:
      • Tax professionals submit data to the Reporting Agent File (RAF) subsystem of IDRS.
      • The IRS contracts with commercial banks for Lockbox Processing Systems (Lockbox) supplies payment data to the Taxpayer Delinquent Account (TDA) subsystem of IDRS.
      • Financial Institutions/Banks send and receive installment agreement payment information to/from the EFT subsystem of IDRS.

   e. Taxpayers (such as the 1040): Yes
   f. Employees (such as the I-9): No
   g. Other: No If Yes, specify:

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

   Tax Administration and Taxpayer Service

D. PII USAGE
14. **What is the specific use(s) of the PII?**

<table>
<thead>
<tr>
<th>Use</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>To conduct Tax Administration</td>
<td>Yes</td>
</tr>
<tr>
<td>To provide Taxpayer Services</td>
<td>Yes</td>
</tr>
<tr>
<td>To collect Demographic Data</td>
<td>No</td>
</tr>
<tr>
<td>For employee purposes</td>
<td>No</td>
</tr>
<tr>
<td>Other:</td>
<td>No</td>
</tr>
</tbody>
</table>

*If other, what is the use?*
E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

<table>
<thead>
<tr>
<th>Yes/No</th>
<th>Who?</th>
<th>ISA OR MOU**</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

<table>
<thead>
<tr>
<th>YES/NO</th>
<th>AUTHORITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Persistent Cookies</td>
<td></td>
</tr>
<tr>
<td>Web Beacons</td>
<td></td>
</tr>
<tr>
<td>Session Cookies</td>
<td></td>
</tr>
</tbody>
</table>

If other, specify:

Other: __________________________

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? No

18a. If Yes, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If Yes, how does the system ensure “due process”? The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to Title 5 USC and Title 26 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

<table>
<thead>
<tr>
<th>Form Number</th>
<th>Form Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1120</td>
<td>US Corporat Income Tax return</td>
</tr>
<tr>
<td>1040</td>
<td>US Individual Income Tax Return</td>
</tr>
</tbody>
</table>

20b. If No, how was consent granted?

Written consent __________________________

Website Opt In or Out option __________________________

Published System of Records Notice in the Federal Register __________________________

Other: __________________________
21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRS Employees:</td>
<td>Yes</td>
</tr>
<tr>
<td>Users</td>
<td>Read Write</td>
</tr>
<tr>
<td>Managers</td>
<td>Read Write</td>
</tr>
<tr>
<td>System Administrators</td>
<td>No Access</td>
</tr>
<tr>
<td>Developers</td>
<td>No Access</td>
</tr>
<tr>
<td>Contractors:</td>
<td>Yes</td>
</tr>
<tr>
<td>Contractor Users</td>
<td>Read Write</td>
</tr>
<tr>
<td>Contractor System Administrators</td>
<td>No Access</td>
</tr>
<tr>
<td>Contractor Developers</td>
<td>No Access</td>
</tr>
<tr>
<td>Other:</td>
<td>No</td>
</tr>
</tbody>
</table>

If you answered yes to contractors, please answer 22a. (All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)

22a. If the contractors or contractor employees act as System Administrators or have “Root Access”, does that person hold a properly adjudicated “High Level” background investigation? Yes

23. How is access to the PII determined and by whom?

   OL5081, IDRS Security Account Administrators

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

   Input and posting validation; end user procedures per IRMs

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? No

25a. If Yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

IDRS is an access or computer application, infrastructure or interface. IDRS does not create, store, and/or manage records as defined under the Federal Records Act (44 U.S.C.) and does not need to be scheduled. Any data within the system itself is considered duplicative of data derived from other systems. The data which is passed through by IDRS is not archived and IDRS itself does not maintain a data log or audit information. Applications that interface with IDRS and have data storage, tracking, and audit information are scheduled and/or will be scheduled independent of IDRS.
26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

Access is granted under control of OL5081 and IDRS Security Account Administrators. Once granted, access is monitored through IDRS Security Reports generated by the Security Access Control System (SACS), external to the IDRS application.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

At rest the data is protected by the security controls in place through the GSS system.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

IDRS sends security audit records to SACS on a continuous basis and meets or exceed IRS & FISMA requirements for security.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)? Yes

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted? 04/30/2013

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

<table>
<thead>
<tr>
<th>SORNS Number</th>
<th>SORNS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>22.060</td>
<td>Automated Non-Master File (ANMF)</td>
</tr>
<tr>
<td>24.030</td>
<td>CADE Individual Master File (IMF)</td>
</tr>
<tr>
<td>24.046</td>
<td>CADE Business Master File (BMF)</td>
</tr>
<tr>
<td>34.037</td>
<td>IRS Audit Trail and Security Records System</td>
</tr>
</tbody>
</table>

Comments
I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

- Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated) | No
- Provided viable alternatives to the use of PII within the system | No
- New privacy measures have been considered/implemented | No
- Other: | No

32a. If Yes to any of the above, please describe:

NA

View other PIAs on IRS.gov