

---

**A. SYSTEM DESCRIPTION**

---

1. Enter the full name and acronym for the system, project, application and/or database. Integrated Data Retrieval System, IDRS

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Integrated Data Retrieval System, IDRS, 906

Next, enter the **date** of the most recent PIA. 8/3/2014

Indicate which of the following changes occurred to require this update (check all that apply).

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>Yes</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

Were there other system changes not listed above? No

If yes, explain what changes were made.

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>Yes</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	Operations & Maintenance (i.e., system is currently operational)

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

---

**A.1 General Business Purpose**

---

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

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.

**B. PII DETAIL**

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or tax identification numbers (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary      Yes On Spouse      Yes On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
No	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

There is no plan to eliminate as these are used as the primary account key.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

---

### **B.1 BUSINESS NEEDS AND ACCURACY**

---

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

Tax administration and taxpayer service.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

Input and posting validation; end user procedures per Internal Revenue Manuals.

---

### **C. PRIVACY ACT AND SYSTEM OF RECORDS**

---

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

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

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

---

**D. RESPONSIBLE PARTIES**

---

10. Identify the individuals for the following system roles. # # Official Use Only

---

**E. INCOMING PII INTERFACES**

---

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA &amp; A?</u>	<u>Authorization Date</u>
Taxpayer Information File (TIF)	No		No	
Treasury Inspector General for Tax Administration (TIGTA)	No		No	
Tax Master File	Yes	07/12/2011	Yes	12/09/2011

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If **yes**, for each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
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	No
The United States Postal Service (USPS)	supplies data to the Taxpayer Delinquent Account (TDA) subsystem of IDRS	No
The Defense Manpower Data Center (DMDC)	supplies data to the TDA subsystem of IDRS	No
The U.S. Department of Agriculture's Federal Payroll Office (FPO)	supplies data to the TDA subsystem of IDRS	No
The Government Sponsored Enterprise (GSE), Federal National Mortgage Association (FNMA)	sends EIN assignments into the EIN RESEARCH AND ASSIGNMENT SYSTEM (ERAS) subsystem of IDRS	No

11c. Does the system receive SBU/PII from State or local agency (-ies)? Yes

If **yes**, for each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

<b><u>Organization Name</u></b>	<b><u>Transmission method</u></b>	<b><u>ISA/MOU</u></b>
State and local Governments	send data to the State Income Tax Levy Program (SITLP) subsystem of IDRS	No
The Employment Commission Data Exchange (ECDE)	supplies data to the Taxpayer Delinquent Account (TDA) subsystem of IDRS	No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

<b><u>Organization Name</u></b>	<b><u>Transmission method</u></b>	<b><u>ISA/MOU</u></b>
Tax professionals	submit data to the Reporting Agent File (RAF) subsystem of IDRS	No
The IRS contracts with commercial banks for Lockbox Processing Systems (Lockbox)	supplies payment data to the Taxpayer Delinquent Account (TDA) subsystem of IDRS	No
Financial Institutions/Banks	send and receive installment agreement payment information to/from the ELECTRONIC FUNDS TRANSFER (EFT) subsystem of IDRS	No

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

<b><u>Form Number</u></b>	<b><u>Form Name</u></b>
1040	Individual Tax Return
1120	US Corporat Income Tax return

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

## **F. PII SENT TO EXTERNAL ORGANIZATIONS**

12. Does this system disseminate SBU/PII? No

## **G. PRIVACY SENSITIVE TECHNOLOGY**

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

---

**H. INDIVIDUAL NOTICE AND CONSENT**

---

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

Data in system is gathered from tax forms---notice is provided in the tax form instructions.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If no, why not? The Internal Revenue Code (IRC) sections 6001, 6011, and 6012(a), and their regulations state that you must file a return or statement with IRS for any tax you are liable for.

19. How does the system or business process ensure due process regarding information access, correction and redress?

The system will allow affective 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.

---

**I. INFORMATION PROTECTION**

---

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level (Read Only/Read Write/Administrator)</u>
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	No	
Developers	No	

Contractor Employees? Yes

<u>Contractor Employees?</u>	<u>Yes/No</u>	<u>Access Level</u>	<u>Background Invest. Level</u>
<b>Contractor Users</b>	<b>Yes</b>	<b>Read and Write</b>	<b>High</b>
<b>Contractor Managers</b>	<b>No</b>		
<b>Contractor Sys. Admin.</b>	<b>No</b>		
<b>Contractor Developers</b>	<b>No</b>		

21a. How is access to SBU/PII determined and by whom? Online 5081, IDRS Security Account Administrators.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?  
Not Applicable

---

## **I.1 RECORDS RETENTION SCHEDULE**

---

22. 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

22b. 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.

---

## **I.2 SA&A OR ECM-R**

---

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 12/21/2016

23.1 Describe in detail the system's audit trail. Audit trails consist of: 10 digit assigned unique employee number, 10-digit case number & Tax period. 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.

---

## **J. PRIVACY TESTING**

---

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 8/1/2017

24.3 If **completed/ or in process**, describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met? We have completed the annual security control assessment



and received the authority to operate, and have completed the disaster table top exercise. We have completed the change request and security impact assessment.

---

**K. SBU Data Use**

---

25. Does this system use, or plan to use SBU Data in Testing? Yes

25a. If **yes**, was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If **yes**, provide the date the permission was granted. 5/25/2017

25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive but Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

---

**L. NUMBER AND CATEGORY OF PII RECORDS**

---

26. Identify the number of individual records in the system for each category:

26a. IRS Employees:	<u>50,000 to 100,000</u>
26b. Contractors:	<u>5,000 to 10,000</u>
26c. Members of the Public:	<u>100,000 to 1,000,000</u>
26d. Other:	<u>No</u>

---

**M. CIVIL LIBERTIES**

---

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

---

**N. ACCOUNTING OF DISCLOSURES**

---

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? Yes

If **yes**, does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required. Yes

---

**End of Report**

---