

---

## A. SYSTEM DESCRIPTION

---

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

---

Date of Approval: March 12, 2014

PIA ID Number: 713

---

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):

Information Returns Processing , IRP

---

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: 50,000 - 100,000

Number of Contractors: Under 5,000

Members of the Public: Over 1,000,000

---

**4. Responsible Parties: ## Redacted Information for Official Use Only**

---

## 5. General Business Purpose of System

---

The Information Returns Processing (IRP) application is a compilation of batch programs with no direct user interface. The IRP System receives data submitted by employers and other third parties (payers) reporting taxpayer income such as wages, pensions, interest and dividends paid during the tax year. This information is validated and stored in the Information Return Master File (IRMF). The information about the payer is stored in the Payer Master File (PMF). IRP provides information technology support to complementary compliance functions allowing the Internal Revenue Service (IRS) to effectively administer the U. S. tax system. Data is sent to the IRP system via a variety of pipeline processes. IRP then attempts to validate all data received, but regardless of the outcome, all data received will be stored on one of several data stores that IRP controls. Upon receipt of an authorized request, IRP performs a data extract and sends requested information internally and externally via MITS-21. Development for IRP is done on a different partition of the ECC-MTB mainframe. IRP is comprised of 12 sub functions, as follows: -- Information Return Master File (IRMF) - The IRMF consists of information return documents that are submitted to the IRS to report taxpayer income (e.g., the 1099-INT, which reports interest earned on items such as Bank accounts). -- IRP Non-filer (IRP NF) - IRP Non-filer identifies individuals who have not filed a Form 1040 for a given tax year, determines whether they should have filed a return, and if so, determines which individuals meet the customer-supplied criteria to receive notices of their failure to file a return. The system uses IMF and IRMF information to identify non-filers. Income from matching IRMF documents is used to compute the IRP income and potential tax for each non-filer. -- Information Returns Document Match Data Assimilation (IRDMDA) - A program run to provide IRP documents (i.e. W-2, 1099K, etc.) to the customers. -- IRP Underreporter (IRP UR) - Identifies taxpayers who have under reported their income by matching IRP documents to the IMF. The purpose of the Underreporter Project (URP) is to match information supplied by taxpayers on Forms 1040, 1040A, and 1040EZ (IMF) with corresponding information supplied by third party payers on Information Returns stored in the IRMF. Discrepancies between the two sources are evaluated for tax consequence, and if appropriate, potential cases are created. Predominant underreported (UR) income type and level of underreporting, as well as other special circumstances categorize the cases. A national inventory exists at ECC-MTB on the IBM mainframe. Automated Underreporter (AUR) campuses order cases from the national inventory. UR case information, extracted IRMF documents, and Return Transaction (RTF) information are supplied to the AUR system. Transaction Code (TC) 922 is posted when cases are ordered to identify potential Underreporters. The master file extracts are generally Assembler Language (ALC) programs run on the IBM mainframe at ECC-MTB. -- IRP Underreporter Backup Withholding (IRP UBWH) - This system issues notices to taxpayers, and their authorized representatives, who are subject to backup withholding, informing them that failure to satisfy tax obligations will result in backup withholding on specific non-wage income. If the taxpayer fails to comply on a timely basis, IRP UBWH notifies all known payers of non-wage income to begin withholding on the taxpayer's account(s) within 30 days. -- Information Returns Processing Input Processing (IRPIP) IRP Validation and Perfection (IRP VAL) - This system processes information returns received via magnetic tape, electronic submission, and paper submission. Input is received primarily from Magnetic Media (MAG) and Generalized Mainline Framework (GMF), but also from the State

Department (Passport documents), W2 Input processing (W2s), and the Social Security Administration (SSA) (1099SSA/RRBs). Payee documents, where Payee Taxpayer Identification Number (TIN) has been successfully validated by TIN Validation, are routed to IRMF. Payee documents, where Payee TIN is not successfully validated, are routed to TIN Perfection to attempt to update and correct the invalid Payee TINs. Payer records are routed to Payer Master File. -- Information Returns Master File Research (IRMFRES) Automated Magnetic Media Processing System (AMMPS) - Automated Magnetic Media Processing System (AMMPS) is used to track, schedule, submit, process and balance the IRP 1099 type data that is sent to ECC-MTB by the transmitting community electronically. Also, Currency Transaction Reports are received from the Currency & Banking Retrieval System (WebCBRS). Passes file to IRP Validation for further processing. -- Social Security Administration-Railroad Retirement Board 1099 (SSA-RRB 1099) - Social Security Administration-Railroad Retirement Board 1099 (SSA-RRB 1099) processes SSA-1099 and RRB-1099 documents received from the Social Security Administration on magnetic media. These documents report on income paid by SSA and RRB to taxpayers. -- Information Returns Transcripts File On Line (IRPTR) - Information Returns Transcript File On Line (IRPTR) is part of the Corporate Files On Line (CFOL) system and is used primarily to display information returns to Integrated Data Retrieval System (IDRS) users. The system uses CICS as a transaction processor. Nationwide access to IRPTR is through the IDRS/Security and Communications System (SACS) telecommunication and security network. Files are accessed via IRS developed CICS command code IRPTR. -- State-Levy Processing (STATE-LEVY) - State-Levy Processing (STATE-LEVY) uses data from the IRMF to provide levy source information to states that request this information. Levy information is provided to the requesting States. -- Taxpayer Delinquency Investigation Supplement On Line (SUPOL) - Taxpayer Delinquency Investigation Supplement On Line (SUPOL) is part of the Corporate Files On Line (CFOL) system. SUPOL provides access to a national database of potential TDI cases. The database contains the Information Return (IRP) document(s) associated with these potential TDI cases. Identification of these nonfilers is done annually by the Information Returns Processing Nonfiler (IRP NF) system. The system uses CICS as a transaction processor. Nationwide access to SUPOL is through the Security and Communications System (SACS) telecommunication and security network. Files are accessed via the CICS command code SUPOL. -- Information Returns Master File Research (IRMFRES) Automated Extensions (AWAX - EAWPMF) - Automated Extensions (AWAX - EAWPMF) receives magnetically and electronically filed requests for extensions of time to file magnetically or electronically for information return documents. This system provides an automated database for waivers and extensions for the filing of information returns from the payer and recipient community. These requests are then approved or denied. Approved payer and recipient requests are sent to the Payer Master File Processing (PMF) through the Extension and Waiver processing (EAWPMF). Payer requests are processed while the recipient requests are used only to create a report. EAWPMF is responsible for posting extensions to the PMF. The purpose of the PMF posting is to prevent issuing penalties for filing IRP documents late (extension related). Processing includes validating extensions, attempting to post valid requests to the Payer Master File, and researching invalid requests. Microfilm Replacement Systems (MRS), Business Master File (BMF) and Individual Master File (IMF) transcript requests are generated for researching unpostable requests. Reports are produced for the Information Returns Branch and for field personnel in the Campuses. Due process is provided outside of the system 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: 09/19/2012

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) No
- System is undergoing Security Assessment and Authorization No

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

Only changes are to the General Business Purpose of System per request from Privacy Office to further clarify sub-systems of IRP, and change to Program Manager, DAA/AO.

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'. 01500000015

## **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
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:

Taxpayers/Public/Tax Systems Yes  
 Employees/Personnel/HR Systems No

*Other Source:*

Other No

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:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	Yes	Yes	Yes
Tax Payer ID Number (TIN)	Yes	Yes	Yes
Address	Yes	Yes	Yes
Date of Birth	Yes	Yes	Yes

**Additional Types of PII:** No

**PII Name On Public? On Employee?**

No No

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

The IRP application contains the following PII data: • Name • SSN • TIN • Address • Date of Birth

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.)

SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. Additional information can be found at these two links: • <http://www.irs.gov/pub/irs-wd/00-0075.pdf> • <http://www.law.cornell.edu/uscode/text/26/6109> Section 7801 and 7803 of the Internal Revenue Code.

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

IRS and Congress have not provided for an alternative means to identify taxpayers.

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

No strategy exists currently for the application

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.

Master files by definition do not have an audit trail. They are defined as having interfaces to systems that maintain their own audit trails. There is no direct access to IRP data. All access is through batch files. The data viewed by authorized IRS employees is a copy of the IMF data loaded into any of a number of other systems that have a user interface. These systems maintain the authentication and authorization required, including the use of audit trail information.

- 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:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA &amp; A?</u>	<u>Authorization Date</u>
Generalized Mainline Framework	Yes	07/06/2011	Yes	09/22/2011
Automated Underreporter	Yes	10/11/2011	Yes	01/30/2012
Business Master File Case Creation Nonfiler Identification Process	Yes	05/01/2012	Yes	10/22/2009
Integrated Production Model	Yes	03/22/2011	Yes	08/01/2011
Integrated Data Retrieval System	Yes	07/12/2011	Yes	12/09/2011
Filing Information Returns Electronically	Yes	10/25/2011	Yes	05/11/2012
Payer Master File	Yes	11/27/2012	Yes	01/22/2013
Individual Master File	Yes	11/10/2009	Yes	11/15/2012
Business Master File	Yes	09/24/2013	Yes	05/23/2013
Generalized Mainline Framework	Yes	07/06/2011	Yes	09/22/2011
Individual Master File	Yes	11/10/2009	Yes	11/15/2012
Business Master File	Yes	09/24/2013	Yes	05/23/2013
Automated Underreporter	Yes	10/11/2011	Yes	01/30/2012
Business Master File Case Creation Nonfiler Identification Process	Yes	05/01/2012	Yes	10/22/2009
Integrated Production Model	Yes	03/22/2011	Yes	08/01/2011
Integrated Data Retrieval System	Yes	07/12/2011	Yes	12/09/2011
Filing Information Returns Electronically	Yes	10/25/2011	Yes	05/11/2012
Payer Master File	Yes	11/27/2012	Yes	01/22/2013

- b. Other federal agency or agencies: No  
 c. State and local agency or agencies: No  
 d. Third party sources: No  
 e. Taxpayers (such as the 1040): <IRS.B.5.E/>  
 f. Employees (such as the I-9): Yes  
 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.

The IRP System receives data submitted by employers and other third parties (payers) reporting taxpayer income such as wages, pensions, interest and dividends paid during the tax year. The name, SSN, TIN Date of Birth, and address are required to identify the recipient of the income. The amount of income is required for various document

matching compliance programs (non-filing and under reporting). IRP provides information technology support to complementary compliance functions allowing the Internal Revenue Service (IRS) to effectively administer the U. S. tax system.

---

**D. PII USAGE**

---

*Authority: OMB M 03-22 & PVR #16, Acceptable Use*

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

To conduct tax administration Yes

To provide taxpayer services Yes

To collect demographic data No

For employee purposes No

Other: No

*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
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? N/A
- 

**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
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 IRP System performs analysis on the data to identify potential compliance issues. The IRP System does not make any adjustments or assessments. The information is reviewed by IRS employees in the Wage & Investment and Small Business/ Self Employed Business Units to correspond with the taxpayer, advising them of the proposed action (either a tax adjustment to an existing assessment or establishing an initial assessment for a tax period). The taxpayers are requested to concur or provide additional information. When applicable, the taxpayer is advised of their statutory appeal rights.
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.

ID	Form Number	Form Name
3041	Form 1040	Individual Tax Return

---

**G. INFORMATION PROTECTIONS**

---

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

---

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

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

	<b>Yes/No</b>	<b>Access Level</b>
IRS Employees:	<u>No</u>	
Users		_____
Managers		_____
System Administrators		_____
Developers		_____
Contractors:	<u>No</u>	
Contractor Users		_____
Contractor System Administrators		_____
Contractor Developers		_____
Other:	<u>No</u>	_____

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?

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

Data access is granted on a need-to-know basis. A potential user must submit a request for access form (Form 5081) to their local management for approval consideration. Users are not permitted access without a signed 5081 form from an authorized management official.

---

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

Validation of SSA data is a joint effort between SSA and IRS. IRS monitors the payer and payee compliance required to report income for accuracy, timeliness and completeness.

---

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? Yes

---

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.

IRP data files are approved for deletion/destruction under a variety of NARA-approved disposition authorities for specific batch programs, and published in IRS Records Control Schedules 19, 28, 29 and 35. This includes various temporary retention periods for Underreporter Backup Withholding (RCS 19, item 64), Validation and Perfection (RCS 19, item 67), Non-filer (RCS 19, item 69), Civil Penalty (RCS 28, item 35), Incorrect Information Penalty (RCS 28, item 147), Information Return Master File (RCS 29, items 85 and 88), and Underreporter (RCS 35, item 31).

---

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

EFTU is the only means of data transmission and encryption for IRP. IRP uses the secure version of Enterprise File Transfer Utility (EFTU) to protect the integrity of transmitted data. IRP relies upon the MITS-21 GSS to protect IRP data at rest as follows: Back Up Tapes: MITS-21 GSS uses the IRS Veritas Netbackup Solution for tape backup. Veritas encrypts all backup tapes utilizing FIPS 140-2 validated encryption. Application Servers: IRM 10.8.1.5.6 (12) states that encryption of data residing on the primary stored devices of IRS information systems (e.g., servers, mainframes) is not required. The MITS-21 environment, in accordance with the IRM, has employed the following due diligence methods for protecting the IRP PII data that resides on the servers:  IRP does not utilize any shares or shared drives.  IRP enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties.  IRP does not routinely print any documents. If required, printing is limited to the specific reason for printing any document.  IRP has had a risk assessment conducted. Security Assessment EFTU is the only means of data transmission and encryption for IRP. IRP uses the secure version of Enterprise File Transfer Utility (EFTU) to protect the integrity of transmitted data. IRP relies upon the MITS-21 GSS to protect IRP data at rest as follows: Back Up Tapes: MITS-21 GSS uses the IRS Veritas Netbackup Solution for tape backup. Veritas encrypts all backup tapes utilizing FIPS 140-2 validated encryption. Application Servers: IRM 10.8.1.5.6 (12) states that encryption of data residing on the primary stored devices of IRS information systems (e.g., servers, mainframes) is not required. The MITS-21 environment, in accordance with the IRM, has employed the following due diligence methods for protecting the IRP PII data that resides on the servers:  IRP does not utilize any shares or shared drives.  IRP enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties.  IRP does not routinely print any documents. If required, printing is limited to the specific reason for printing any document.  IRP has had a risk assessment conducted. Security Assessment Services has previously completed a Security Impact Analysis and will conduct a new SIA as part of the current SA&A cycle.  The IRP SSP is being updated as part of the current SA&A to reflect the encryption utilized by the MITS-21 environment to protect PII data.  Physical security is an inherited control by IRP at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan.

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

see 26.

---

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.

Continuous Monitoring (eCM) is performed annually to determine if selected System Security Plan (SSP) controls are operating as intended. The Security Assessment and Authorization (SA&A) process is conducted on a three year cycle whereby all application information and control descriptions are updated and tested to ensure that the controls continue to work properly in safeguarding the PII. Findings from the SA&A are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings.

---

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? No

---

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

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

---

#### **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.

SORN Number	SORN Name
Treasury/IRS 22.061	Information Return Master File
Treasury/IRS 24.030	IMF
Treasury/IRS 34.037	IRS Audit Trail and Security Records System

## 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