

---

**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 Submission: Jun. 13, 2012

PIA ID Number: 202

---

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):

Photocopy Refunds Program, PHOREF

---

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: Not Applicable

Number of Contractors: Not Applicable

Members of the Public: 100,000 – 1,000,000

---

4. Responsible Parties:

---

N/A

---

5. General Business Purpose of System

---

The Photocopy Refunds Program (PHOREF) application was designed to assist taxpayers in dealing with issues regarding the refund of fees paid by taxpayers for photocopies of their tax return forms. A photocopy user fee is the fee that is paid to the Internal Revenue Service (IRS) for providing a taxpayer with a copy of their tax return. The IRS charges a \$57 fee for each photocopy of a return but transcripts of tax information are provided free of charge. Taxpayers prepay the fee of \$57 for each tax return photocopy requested when submitting a Form 4506, Request for Copy of Tax Form. Requests are made for photocopies of tax returns. The fee is refunded to the taxpayer if the IRS later determines that it cannot provide a photocopy of the requested tax return. The Returns and Income Verification Services (RAIVS) function controls the Form 4506 and initiates refunds if copies of tax returns cannot be provided to taxpayers. Refunds are issued using the PHOREF program because the photocopy user fee payments are not recorded separately on IRS Master File (MF) accounts. Refunds are generally issued weekly. Taxpayers may request a copy of their tax return to be disclosed to a third party. The request, or consent, must be in the form of a written document and signed and dated by the taxpayer who filed the return. Generally, taxpayers use a Form 4506 when making these types of requests. The IRS centers process these written requests under the provisions of the Internal Revenue Code (IRC) Section 6103, Confidentiality and Disclosure of Returns and Return Information. PHOREF provides employees in the RAIVS unit the ability to issue photocopy fee refunds by inputting data pertinent to each individual case. The data entered is Social Security Number (SSN), name, address, refund amount, refund date, caseworker's Integrated Data Retrieval System (IDRS) number, and appropriate remarks regarding the case.

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: 07/01/2009

---

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 Yes

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

Upgraded from Oracle 10g to 11g in 2011. In January 2010 PHOREF converted from Informix to Oracle.

**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'. 015-45-01-12-02-2514-00**

**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:**

Taxpayers/Public/Tax Systems Yes

Employees/Personnel/HR Systems No

Other No

Other Source: \_\_\_\_\_

**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	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: Yes

<u>PII Name</u>	<u>On Public?</u>	<u>On Employee?</u>
3rd Party Name & Address & Phone Number	Yes	No
SEID	No	Yes

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

Name SSN TIN Address EIN Third Party Name, address, and telephone number SEID

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.)**

Internal Revenue Code (IRC) 6109

---

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 provided

---

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 currently exists.

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.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*?

---

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: No

If Yes, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: No

If yes, the third party sources that were used are:

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): No

g. Other: Yes If Yes, specify: IRS Form 4506

---

### 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 data collected is used for the purpose of identifying the taxpayer and processing their photocopy fee refund request. The actual refund check fee is mailed from Financial Management Services (FMS) to the taxpayer.

---

### 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 No

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.) Yes

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

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	Yes	FMS. However, PHOREF does not directly interconnect with FMS. IRS uses General Support Systems(GSS) to exchange information outside the IRS.	Yes
State and local agency (-ies)	No		
Third party sources	No		
Other:	No		

\*\* 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:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	_____

*If other, specify:*

---

**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? Not Applicable

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? Not Applicable

19a. If Yes, how does the system ensure "due process"?

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.

No forms found.

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:	_____

---

**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

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:

	Yes/No	Access Level
IRS Employees:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Write</u>
System Administrators		<u>Read Only</u>
Developers		<u>Read Only</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other: <u>Database Administrator</u>	<u>Yes</u>	<u>Read Only</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?

PHOREF management determines employee access. Access to the PHOREF application is obtained by completing an Online 5081 (OL5081) request. The form contains information on the permissions or roles assigned to the account. Upon receiving approval, the DBA creates an account for the requesting new user and an existing PHO4 user (prompted by the new user's manager) will add the new user to the application and set the new user's role.

---

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

The PHOREF application checks information inputs for accuracy, completeness, validity, and authenticity of information as close to the point of origin as possible. PHOREF employs rules to check the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to verify that inputs match specified definitions for format and content. The application prescreens inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands. The RAIVS Unit has a business process in place where RAIVS Unit users input data from Form 4506 into the database. The unit lead verifies for accuracy, timeliness, and completeness before a report of all records is printed and sent to the Accounting Unit for further validation.

---

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.

PHOREF data is approved for destruction 6 years, 3 months after the fiscal year in which the refund was issued (Job No. N1–58–09–71). This data disposition, along with retention instructions for PHOREF inputs, outputs and system documentation, will be published in IRM/Records Control Schedule 1.15.29 for Tax Administration – Wage and Investment Records, item 428 when next updated.

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.

---

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

Enterprise File Transfer Utility (EFTU) is the only means of data transmission and encryption for PHOREF. PHOREF uses the secure version of EFTU to protect the integrity of transmitted data.

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

PHOREF relies upon the MITS–24 GSS to secure data at rest. The MITS–24 GSS protects PHOREF data at rest as follows: PHOREF does not utilize any share drives. PHOREF enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties. PHOREF does not routinely print any documents. If required, printing is limited to the specific reason for printing any document. PHOREF 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. Physical security is an inherited control by PHOREF at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan.

---

**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? Not Applicable**

---

**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.**

**SORNS Number**

**SORNS Name**

IRS22.054

Subsidiary Accounting Files

IRS24.030

Individual Master File (IMF), Taxpayer Services

IRS24.046

Business Master File (BMF), Taxpayer Services

IRS34.037

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)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>No</u>
Other:	<u>No</u>

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

NA

[View other PIAs on IRS.gov](#)