
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: **04/08/2014** PIA ID Number: **821**

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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

Federal Payment Levy Program, FPLP

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: Over 1,000,000

4. Responsible Parties:

N/A

5. General Business Purpose of System

Federal Payment Levy Program (FPLP) is a systemic collection enforcement tool application where certain delinquent taxpayers are match and levied for their Federal Payments disbursed by Treasury's Bureau of Fiscal Service (BFS)(Formerly Financial Management Service (FMS)). Each week, IRS Financial Systems creates a file of certain balance due accounts and transmits the file to BFS' Treasury Offset Program (TOP). BFS transmits a weekly file back to IRS (received by Unpaid Assessments (UA)) listing those who matched. FPLP will subsequently transmit levies on accounts that had matched. On Social Security benefit payment matches, FPLP will send a transaction to the Individual Master File (IMF) which results in a special pre-levy collection notice to those taxpayers, copies of the notices are also transmitted to SSA for tax administration purposes. 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: 03/03/2009

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 No

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

No Changes.

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'. 015-000000116

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	No
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: No

PII Name On Public? On Employee?

No No

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

Taxpayer:

- Taxpayer Identification Number (TIN)
- Master File Account Code (MFT)
- Tax Period (TXPD)
- Balance Due
- Address Other Payment amount
- Payer information

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.)

IRS Code section 6103 (k)(8)

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

There are no alternative solution at this time.

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

There are no mitigation strategy at this time.

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.

FPLP audit trail protection is provided by the Modernization and Information Technology Service (MITS) - 21 General Support System (GSS), System of Records Notice Number: Treasury/IRS 34.037

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

IMF No No

BMF No No

b. Other federal agency or agencies: Yes

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

Bureau of Fiscal Services (BFS), Social Security Administration (SSA).

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): No

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.

For TIN, MFT, TXPD; each is a piece that contributes to creating a unique debt number balance due, so BFS knows how much to send. Address: to where to send follow-up notice Payment amount: Amount that is levied and credited on the delinquent taxpayer account. Payor information: Income/asset information of delinquent taxpayer from collection source. The data is stored in the delinquent taxpayer account record for future collection enforcement information.

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	<u>Yes</u>
To provide Taxpayer Services	<u>Yes</u>
To collect Demographic Data	<u>No</u>
For employee purposes	<u>No</u>

If other, what is the use?

Other:	<u>No</u>	<u>_____</u>
--------	-----------	--------------

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	Bureau of Fiscal Service (BFS) Treasury Offess Program (TOP) and Social Security Adminisitration (SSA)	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? Yes

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

IRS sends the taxpayer a certified return receipt requested Collection Due Process notice advising taxpayers of their appeals rights before any collection action is taken. Legislation allows collection on federal contractors before 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 Only</u>
Managers		<u>Read Only</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>BFS and SSA</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?

FPLP is a batch program with restricted Internal IRS access and no end-user capabilities. There are Information Technology (IT) programmers who work on FPLP providing software maintenance support. The IT programmers do not have write permissions to the production application. Support personnel at the Enterprise Computing Center in Martinsburg (ECC-MTB) also have access to the application in mainframe to provide processing operations support, computer facilities, equipment and data storage on the MITS 21 (IBM Master File) General Support System which has its own security support plan. This is in compliance with the Privacy Act of 1974.

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

Each data element is taken directly from the current week's IRS Master File tapes. Data received from BFS is certified by the Federal agency providing it to BFS. Validity and accuracy of that data is the responsibility of the systems that provide data to FPLP. There is no direct user input to the FPLP system, All data is received from other systems, The forms are input into the feeder systems (IDRS/Masterfile). FPLP receives the data from the MITS-21 GSS. To ensure no data is lost, the Log Accounting Report System (LARS) is used to ensure that the number of records sent matches the number of records received by FPLP.

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.

FPLP taxpayer collection notices are scheduled under Records Control Schedule (RCS) 29, Item 38 for Certified and Registered Mail Records (disposition instructions published in Document 12990).

FPLP delinquent taxpayer account information is only necessary to maintain until it is transferred to/verified by IMF for recordkeeping purposes and other outside data stakeholders.

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.

The PII data is secured at ECC-MTB and data is storage on the MITS 21 General Support System.

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

NA Since the data is secured at ECC-MTB and controlled by MITS 21 an OL5081 log on is required to access the data. Also permission is granted to authorized users. Data is never transported.

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.

Monitoring and evaluation activities is performed by MITS 21.

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)? No

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

IRS 34.037

IRS Audit Trail and Security Records System

IRS 26.019

Taxpayer Delinquent Accounts

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)	<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](#)