

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

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: June 23, 2014

PIA ID Number: **867**

1. What type of system is this? Legacy

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

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

Integrated Procurement System, IPS

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: Under 50,000

Number of Contractors: Under 5,000

Members of the Public: Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

IPS (Integrated Procurement System) is a software application whose primary purpose is to automate the acquisition process. The system provides a flexible and efficient way to prepare, approve, fund, and track requisitions for the delivery of goods and services. The IPS application tracks all incoming commitment requests and captures the information necessary to make awards (such as purchase orders, delivery orders, task orders, contract awards, and interagency agreements and modifications). This application is also responsible for printing pertinent award documents and reports which are required for integrated internal and external management and operation. Due process is provided by applicable federal procurement statutes and regulations.

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: 09/21/2011

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) No
 - System is undergoing Security Assessment and Authorization No
-

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

N/A

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'. 015-000000047

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	<u>No</u>	
Employees/Personnel/HR Systems	<u>Yes</u>	
Other	<u>Yes</u>	<i>Other Source:</i> <u>Federal Contractor Registration System</u>

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? On Employee?</u>	
Employee ID	No	Yes
Employee SEID	No	Yes
Employee Work Address	No	Yes
Employee Work Email	No	Yes
Employee Work Phone Number	No	Yes
Vendor TIN/ Social Security Number	Yes	No
Vendor Bank Account Number and Bank Routing Number	Yes	No
Purchase Card Account Number	Yes	No

10a. What is the business purpose for collecting and using the SSN ?

The purpose for collecting and using the SSN is for Procurement Acquisitioning and processing of financial payments.

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.

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 currently no plans to mask or truncate the SSN.

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

There is currently no plan to eliminate the use of TIN/SSN for vendor data.

Describe the PII available in the system referred to in question 10 above.

The information that is stored in the system is: Employee ID Employee SEID Employee Work Address Employee Work Email Employee Work Phone Number Vendor TIN/ Social Security Number (SSN) – Used to group vendors. Sent to IFS for issuance of 1099. Vendor Bank Account Number and Bank Routing Number – Sent to IFS. Used for Electronic Funds Transfer (EFT) payment. Purchase Card Account Number – Associated with each individual. Used for making purchases with the IRS

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 Trail Information: Information is used for tracking User activity in the application: User Identification (ID) User Type System Event Type Event ID Tax Filer Taxpayer Identification Number (TIN) Session ID Source Address Return Code Error Message Timestamp Variable Data Tax Period MFT Code

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: No
- b. Other federal agency or agencies: Yes
- c. State and local agency or agencies: No
- d. Third party sources: No
- 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.

The data is collected in support of IRS Procurement Activities.

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>No</u>
To provide taxpayer services	<u>No</u>
To collect demographic data	<u>No</u>
For employee purposes	<u>No</u>

Other:

Yes

If other, what is the use?

Support of Procurment
Realated Activities

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?
If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies	_____	_____
Web Beacons	_____	_____
Session Cookies	_____	_____
Other:	_____	<i>If other, specify:</i> _____

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"?

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 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? No
- 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	<u>No</u>
Website Opt In or Out option	<u>No</u>
Published System of Records Notice in the Federal Register	<u>No</u>
Other: <u>Online 5081 is used to request access to IPS</u>	<u>Yes</u>

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 Write</u>
Developers		<u>No Access</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></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?

Access to data is controlled by role based access. The privileges granted to each role are based on a need-to-know basis. Requests for role membership will be managed using the OL5081 system. These roles will govern the nature of data available to different users based on administrative requirements. Each OL5081 role request must be approved by the requestor's immediate manager and any additional approvals required based on the role requested.

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

Prior to release to the production environment, extensive testing is performed to verify the accuracy, timeliness and completeness of the data elements. Format masks, edit checks and referential integrity checks are also used to ensure accuracy 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.

The records within IPS are financial records. Data retention conforms to CFR 4.804-5 requirements, and the National Archives and Records Administration's (NARA) General Records Schedule (GRS) 6, Item 1 (IRS RCS 1.15.43, Item 1) for Accountable Officers' Files. NARA approves destruction of recordkeeping copies of this financial data 6 years, 3 months after period covered by account.

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.

IPS utilizes a single sign on (SSO) capability using the IRS Active Directory (AD). All sensitive PII data is protected by the IPS application and only authorized application users have access permissions to view and/or modify application data.

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

Individual activities within the system are monitored for adherence to policy and controls, and detection of suspect activity. The information collected is only used for tracking user activity in the application.

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.

Individual activities within the system are monitored for adherence to policy and controls, and detection of suspect activity. The information collected is only used for tracking user activity in the application.

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?

05/21/2014

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.

Treasury .009	Treasury Financial Management Systems
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:

Not Applicable