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: Aug 20 2014 7:18PM PIA ID Number: **1032**

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):

GHW Workload Services Database, N/A

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:	Under 100,000

4. Responsible Parties:

NA

5. General Business Purpose of System

Collection of public tax relevant data: (1) retrieve names of taxpayers in the global high wealth population and research tax-relevant information from publicly available sources, (2) save research findings in taxpayer-specific information files and record findings, and (3) analyze whether findings result in the need for a more in-depth risk assessment. 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: 11/10/2010

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 material changes have occurred to the system since the last PIA.

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'. NA

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 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	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

No Other PII Records found.

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

The work process supported requires that information collected be associated with tax returns, and the SSN is needed to correctly identify the taxpayer and obtain the tax return and tax return data.

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.)

IRC 6103, 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)

We will continue to address the need to retain the SSN based on experience with this system. Currently, the work process supported requires that information collected be associated with tax returns, and the SSN is needed to correctly identify the taxpayer and obtain the tax return and tax return data.

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

We will continue to address the need to retain the SSN based on experience with this system. Currently, the work process supported requires that information collected be associated with tax returns, and the SSN is needed to correctly identify the taxpayer and obtain the tax return and tax return data.

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

Public information such as names, addresses and research on business and financial dealings will be associated with taxpayers within the global high wealth taxpayer population.

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.

For LB&I GHW Server, the following minimum set of operations is audited for successful and unsuccessful execution: This is done by reviewing the SQL Error Logs weekly. Unless we find an intrusion, then SQL Logs will be audited daily. DBA Runs SQL Profiler to also track the events daily and will review the SQLProfiler weekly. DBA runs an Audit Trace file. SQL Trace includes but not limited to the following: • The DBA ensures that the creation, alteration, or deletion (drop) of database accounts is audited • The DBA ensures that the creation, alteration, or deletion (drop) of any database system storage structure is audited • The DBA ensures that the creation, alteration, or deletion (drop) of database objects is audited • The DBA ensures that the creation, alteration, or deletion (drop) of database tables is audited • The DBA ensures that the creation, alteration, or deletion (drop) of database indexes is audited • The DBA ensures that enabling and disabling of audit functionality is audited and reviewed • The DBA ensures that granting and revoking of database system level privileges is audited and reviewed • The DBA ensures that any action that returns an error message because the object referenced does not exist is audited and reviewed • The DBA ensures that any action that renames a database object is audited and reviewed. • The DBA ensures that any action that grants or revokes object privileges from a database role or database account is audited • The DBA ensures that all modifications to the data dictionary or database system configuration are audited • The DBA ensures that all database connection failures are audited. Where possible, the DBA ensures that both successful and unsuccessful connection attempts are audited. All connections performed to maintain or administer the database are audited. All DBA operations are audited. At a minimum, the DBA connection is audited and the following list of DBA activities is reported: • Database startup • Database shutdown • Database online backup • Database archiving • Database performance statistics collection • The DBA shall ensure that all database connections used to perform the above listed DBA actions are audited. DBA will document the dates of when the review of the SQL Error Logs, SQL Profiler Logs, and Audit Events are done. See LMSBDCS_SQLLOGS_Review.xls If DBA finds an intrusion; they open an ITAMS Ticket and assign the ticket to EOPS-ECC-SMO-OSM&R Unit 1 (security) to have them look at the events in audit logs. DBA will monitor the ticket and put the result of this ticket in the LMSBDCS_SQLLOGS.xls with its findings. The DBA will notify the backup DBA when they are out of the office for a period of 1 week, so that the backup DBA can do the auditing.

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
Individual Return Transaction File/Compliance Data Warehouse	Yes	03/24/2008	No	

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): 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.

To aid in the risk assessment process for the Global High Wealth taxpayer population. The information obtained may cause the taxpayer to ascend or descend in terms of audit risk.

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	No	
To collect demographic data	No	
For employee purposes	No	
		If other, what is the use?
Other:	No	

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

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)			
State and local agency (-ies)			
Third party sources			
Other:			

** 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		
		If other, specify:
Other:		

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? Yes

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

Form Number	Form Name
1040	Individual Income Tax Return

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:	Yes	
Users		Read Write
Managers		Read Write
System Administrators		Read Write
Developers		Read Write
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

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?

Global High Wealth Workload Services Manager of Compliance Analysts will be responsible for hiring and training employees who will have access to the data.

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

Each data element will be reviewed by the Compliance Analyst Manager as well as by one of the Risk Assessment Analysts in Workload Services for tax relevance, 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? No

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.

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.

A request for records disposition authority for GHW will be drafted with the assistance of the IRS Records and Information Management (RIM) Program Office for National Archives approval. GHW system owners are currently considering minimum data retention of five years.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
Compliance Analysts in the Global High Wealth Workload Services Team will be required to submit an OL5081 requesting access to the Detroit Test Domain (OL5081 application name: LAB-DDT-Development (LAB-LAN)). Once approved, user will be added to a 'project' security group based on level of permission requested: (BAG-LMSB-HiWealth Admin or BAG-LMSB-HiWealth User). GHW Server: The project security group is added to the SQL Server security login credentials. SQL DBA will add user account to the SQL UserTable and supply mapping instructions to end user. User SEID must be added to or exist in the SQL UserTable for end user to see database content. GHW Virtual Workstations: End user will be accessing database interface via a Virtual Workstation also housed in the Detroit Test Domain. ODBC Connection configured on virtual workstation. Also, the project security group is added to the 'local users and group' in the Microsoft Computer Management Console, as well as Remote Desktop permissions granted.

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

Compliance Analysts in the Global High Wealth Workload Services Team will be required to submit an OL5081 requesting access to the Detroit Test Domain (OL5081 application name: LAB-DDT-Development (LAB-LAN)). Once approved, user will be added to a 'project' security group based on level of permission requested: (BAG-LMSB-HiWealth Admin or BAG-LMSB-HiWealth User). GHW Server: The project security group is added to the SQL Server security login credentials. SQL DBA will add user account to the SQL UserTable and supply mapping instructions to end user. User SEID must be added to or exist in the SQL UserTable for end user to see database content. GHW Virtual Workstations: End user will be accessing database interface via a Virtual Workstation also housed in the Detroit Test Domain. ODBC Connection configured on virtual workstation. Also, the project security group is added to the 'local users and group' in the Microsoft Computer Management Console, as well as Remote Desktop permissions granted.

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? No

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

For LB&I GHW Server, the following minimum set of operations is audited for successful and unsuccessful execution: This is done by reviewing the SQL Error Logs weekly. Unless we find an intrusion, then SQL Logs will be audited daily. DBA Runs SQL Profiler to also track the events daily and will review the SQLProfiler weekly. DBA runs an Audit Trace file. SQL Trace includes but not limited to the following: • The DBA ensures that the creation, alteration, or deletion (drop) of database accounts is audited • The DBA ensures that the creation, alteration, or deletion (drop) of any database system storage structure is audited • The DBA ensures that the creation, alteration, or deletion (drop) of database objects is audited • The DBA ensures that the creation, alteration, or deletion (drop) of database tables is audited • The DBA ensures that the creation, alteration, or deletion (drop) of database indexes

is audited • The DBA ensures that enabling and disabling of audit functionality is audited and reviewed • The DBA ensures that granting and revoking of database system level privileges is audited and reviewed • The DBA ensures that any action that returns an error message because the object referenced does not exist is audited and reviewed • The DBA ensures that any action that renames a database object is audited and reviewed. • The DBA ensures that any action that grants or revokes object privileges from a database role or database account is audited • The DBA ensures that all modifications to the data dictionary or database system configuration are audited • The DBA ensures that all database connection failures are audited. Where possible, the DBA ensures that both successful and unsuccessful connection attempts are audited. All connections performed to maintain or administer the database are audited. All DBA operations are audited. At a minimum, the DBA connection is audited and the following list of DBA activities is reported: • Database startup • Database shutdown • Database online backup • Database archiving • Database performance statistics collection • The DBA shall ensure that all database connections used to perform the above listed DBA actions are audited. DBA will document the dates of when the review of the SQL Error Logs, SQL Profiler Logs, and Audit Events are done. See LMSBDCS_SQLLOGS_Review.xls If DBA finds an intrusion; they open an ITAMS Ticket and assign the ticket to EOPS-ECC-SMO-OSM&R Unit 1 (security) to have them look at the events in audit logs. DBA will monitor the ticket and put the result of this ticket in the LMSBDCS_SQLLOGS.xls with its findings. The DBA will notify the backup DBA when they are out of the office for a period of 1 week, so that the backup DBA can do the auditing.

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?

10/26/2010

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
42.021	Compliance Programs and Projects Files
24.030	CADE Individual Master File
24.046	CADE Business Master File
34.037	IRS Audit Trail and Security 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