Date of Approval: September 19, 2017   PIA ID Number: **2836**

___

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. <u>GHW Workload Services Database, N/A</u>

2. Is this a new system? <u>No</u>

> 2a. If **no**, is there a PIA for this system? <u>Yes</u>
>
> > If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA. <u>#931</u>
> >
> > Next, enter the **date** of the most recent PIA. <u>08/22/2014</u>
> >
> > Indicate which of the following changes occurred to require this update (check all that apply).

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

> > Were there other system changes not listed above? <u>No</u>

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? <u>No</u>

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

   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 the taxpayer-specific information files and record findings, and (3) analyze whether findings result in the need for a more in-depth risk assessment.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

   6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or tax identification numbers (i.e. last 4 digits, etc.)? Yes

      If **yes**, check who the SSN (or tax identification number) is collected on.

   Yes   On Primary   No   On Spouse   No   On Dependent

      If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

   Yes   Social Security Number (SSN)
   Yes   Employer Identification Number (EIN)
   No   Individual Taxpayer Identification Number (ITIN)
   No   Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
   No   Practitioner Tax Identification Number (PTIN)

      Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

      The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The GHW database system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) <u>Yes</u>

If **yes**, specify the information.

On Primary		On Spouse	On Dependent	Selected	PII Element
Yes	Name		Yes	Yes	No
Yes	Mailing address		No	No	No
No	Phone Numbers		No	No	No
No	E-mail Address		No	No	No
No	Date of Birth		No	No	No
No	Place of Birth		No	No	No
No	SEID		No	No	No
No	Mother's Maiden Name		No	No	No
No	Protection Personal Identification Numbers (IP PIN)		No	No	No
No	Internet Protocol Address (IP Address)		No	No	No
No	Criminal History		No	No	No
No	Medical Information		No	No	No
No	Certificate or License Numbers		No	No	No
No	Vehicle Identifiers		No	No	No
No	Passport Number		No	No	No
No	Alien (A-) Number		No	No	No
No	Financial Account Numbers		No	No	No
No	Photographic Identifiers		No	No	No
No	Biometric Identifiers		No	No	No
Yes	Employment (HR) Information		No	No	No
Yes	Tax Account Information		Yes	Yes	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates?   <u>Yes</u>

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system?   <u>No</u>

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
Yes	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner?   <u>Yes</u>

B.1 BUSINESS NEEDS AND ACCURACY

---

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

   <u>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.</u>

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

   <u>Each data element will be reviewed by the Compliance Analysts Manager as well as by one of the Risk Assessment Analysts in Workload Services for tax relevance, accuracy, timeliness and completeness.</u>

C. PRIVACY ACT AND SYSTEM OF RECORDS

---

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system?   <u>Yes</u>

   9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual?   <u>Yes</u>

   If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system?   <u>Yes</u>

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
IRS 42.021	Compliance Programs and Projects Files
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File
IRS 34.037	Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act?   Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies?   Yes

    11a. If **yes**, does the system receive SBU/PII from IRS files and databases?   Yes

        If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Individual Return Transaction File/Compliance Data Warehouse	Yes	03/18/2016	No	

    11b. Does the system receive SBU/PII from other federal agency or agencies?   No

    11c. Does the system receive SBU/PII from State or local agencies?   No

    11d. Does the system receive SBU/PII from other sources?   No

    11e. Does the system receive SBU/PII from **Taxpayer** forms?   Yes

     If **yes**, identify the forms

Form Number	Form Name
1040	Individual Return
1065	Partnership Return
1120S	S-Corporation Return

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)?   No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII?   No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels?   No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?   No

15. Does the system use cloud computing?   No

16. Does this system/application interact with the public?   No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information?   Yes

   17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
   The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. All other information is derived from publicly derived sources.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?   Yes

   18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
   All individuals have the right to decline to provide information. However, they may be subject to Examination or Deficiency procedures, at which time they are provided applicable notices, such as Your Appeals Rights and How to Prepare a Protest.

19. How does the system or business process ensure due process regarding information access, correction and redress?
   Due process is provided pursuant to 26 USC.

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

   IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees?   Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Read and Write
Developers	Yes	Read and Write

Contractor Employees?   No

21a. How is access to SBU/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. . User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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

22b. 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 a minimum data retention of five years

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)?   No

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?   Yes

23.1 Describe in detail the system's audit trail.   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 Structured Queried Language (SQL) Logs will be audited daily. DBA Runs SQL Profiler to also track the events daily and will review the SQLProfiler weekly. Database Administrator runs an Audit Trace file. SQL Trace

includes but not limited to the following: • The DBA ensures that the creation, alteration, or 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

    24c. If **no**, please explain why. Not applicable

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing?   No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

    26a. IRS Employees: Not Applicable
    26b. Contractors: Not Applicable
    26c. Members of the Public: Under 100,000
    26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?   No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people?
Yes

> If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. <u>The only way the system is used is to determine the location of the individual and or business for examination assignment only after a risk assessment has taken place and the taxpayer was selected as a result of the risk assessment.</u>

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? <u>No</u>

End of Report