

Date of Approval: **December 17, 2020**

PIA ID Number: **5362**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Global High Wealth Database, GHWDATABASE

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Global High Wealth Services Database. PIA # 2836

What is the approval date of the most recent PCLIA?

9/14/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

None

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

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 finding , and (3) analyze whether findings results in the need for a more in-depth risk assessment.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

Global High Wealth is required by the IRM to identify taxpayers and their related entities they control for the Global High Wealth population and document the risk assessment on those taxpayers and related entities.

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.

Employer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Are there other types of SBU/PII used in the system?

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

PII about individuals for Bank Secrecy Act compliance 31 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

- 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

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Individual Return Transaction File/Compliance Data Warehouse

Current PCLIA: Yes

Approval Date: 9/16/2020

SA&A: Yes

ATO/IATO Date: 5/29/2018

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 5362 Form Name: Global High Wealth Database

Form Number: Form 1040 Form Name: US Individual income tax return

Form Number: Form 1120-S Form Name: U.S. Income Tax Return for an S Corporation

Form Number: Form 1065 Form Name: U.S. Return of Partnership Income

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

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

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

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

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.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

Due process is provided pursuant to Title 26 United States Code (USC).

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Read Write

Developers: Read Write

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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

RCS 26 Item 16-Information Gathering Records and Projects. Evidence of non-compliance in a particular area or group uncovered by post employees and submitted to headquarters as a recommended examination or criminal investigation project. (Job No. NI-58-88-5, Item 17)- Destroy 2 years after case is closed or when no longer needed, whichever is earlier.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

For Large Business and International (LB&I) GHW Server, the following minimum set of operations is audited for successful and unsuccessful execution: This is done by reviewing the Structured Queried Language (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. Database Administrator 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 Database Administrator (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. 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.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

Not applicable

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

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

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.

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.

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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?

No