

Date of Approval: **August 24, 2023**

PIA ID Number: **7238**

SYSTEM DESCRIPTION

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

Research, Applied Analytics & Statistics Offshore, D&B

Is this a new system?

Yes

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

Research, Applied Analytics & Statistics Portfolio Review Board

Current ELC (Enterprise Life Cycle) Milestones:

Vision & Strategy/Milestone 0

Project Initiation/Milestone 1

Preliminary Design/Milestone 3

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

Yes

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.

The IRS Research, Applied Analytics & Statistics (RAAS) Offshore Tax Compliance Modeling project is a RAAS and Large Business and International (LB&I) joint effort to identify emerging offshore noncompliance through a series of models. The key component of this effort is to link business names and addresses from IRS data with third party (Dun and Bradstreet - (D&B)) data within the third party's system. In general, IRS data only provides the service so much visibility on US related individual and business interests abroad. In order to improve our visibility, we have contracted with Noblis (who has partnered with D&B). D&B maintains an extensive relational database for global businesses. Linking to this database allows us to see the structure and location of a given US related business's offshore interests. An analysis and tracking of the offshore structures at the firm level and in aggregation will be insightful for risk modeling as well as help improve our understanding of

emerging offshore risks. We plan to send business name and address data from IRS data securely to D&B. D&B will use their proprietary business matching algorithms to link the IRS data to their relation database for global businesses. After linking, D&B may generate risk measures using existing proprietary flags as well as develop custom measures. Once complete, D&B will securely transfer the linked data back to the IRS where it will be stored on the Compliance Data Warehouse (CDW). Please note that we explored not sending IRS data to D&B and instead having them transfer data to the IRS and perform the linking within IRS systems. This solution was not feasible. D&B considers their linking algorithm as well as some of their data sources used to facilitate the link as proprietary.

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?

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

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.

Proprietary Data - Business information that does not belong to the IRS.

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)

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.

SBU/PII (Name/Address/EIN) currently stored on existing IRS systems will be sent to a third party to link to their proprietary data. The purpose of this portion of the effort is to match IRS data to third party data using SBU/PII data because the third-party data does not contain EIN, except for larger corporations. EINs - many larger corporations have their EINs listed in the public domain (SEC disclosures). Including EIN in the linking criteria, when possible, improves the validity of the match with the third-party data. Business Name and Address - linking with third party data is not possible without name and address.

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

The SBU/PII used is currently stored in existing IRS systems, so its accuracy/completeness is as good as the service currently has. If relevant, the third party has proprietary techniques to estimate the quality of the linking that they perform.

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

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: CDW
Current PCLIA: Yes
Approval Date: 9/16/2020
SA&A: Yes
ATO/IATO Date: 5/10/2022

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?

No

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: CDW
Current PCLIA: Yes
Approval Date: 9/16/2020
SA&A: Yes
ATO/IATO Date: 5/10/2022

Identify the authority.

Under Authority 6103(n)

For what purpose?

The contractor will link the data to their proprietary data then send it back to the IRS.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

5/1/2013

Please identify the ownership of the CSP data.

Third Party

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

3rd Party

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

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?

Privacy act notice provided for 1040, Information collected for tax administration pursuant to IRC.

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

No

Why not?

Information required for tax administration pursuant to IRC, title 26.

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

Due process provided pursuant to IRC.

INFORMATION PROTECTION

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

Contractor Owned and Operated

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

IRS Contractor Employees

Contractor Users: Read Write

Contractor System Administrators: Administrator

How is access to SBU/PII determined and by whom?

Only D&B employees that have been onboarded and have Business Entitlement Access Request System (BEARS) permissions to access this data in the CDW environment will access this data in the D&B environment.

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.

CDW data is approved for destruction 10 years after end of the Processing Year or when no longer needed for operational purposes, which-ever is later (Job No. N1-058-10-007). All CDW records will be erased or purged from the system in accordance with approved retention periods. Records generated will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedules (RCS) 27, item 54 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

SA&A OR ASCA

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

Yes

What date was it completed?

5/9/2023

Describe the system's audit trail.

The contractor works with several federal agencies and has the capability to implement the necessary audit trail functionality.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

This system is managed by our contractor and given the nature of this work we believe a test plan is not applicable. If one is necessary, then guidance on what needs to be done is needed.

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: More than 1,000,000

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?

No

Does computer matching occur?

Yes

Does your matching meet the Privacy Act definition of a matching program?

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