Date of Approval: **May 07, 2021**

PIA ID Number: **5958**

SYSTEM DESCRIPTION

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

Information Returns Database, IRDB

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?

INFORMATION RETURNS DATABASE (IRDB)

What is the approval date of the most recent PCLIA?

5/3/2018

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.

Data Delivery Services (DDS)

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?

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.

Information Returns Database (IRDB) is a production system within the ACA (Affordable Care Act) program and is part of the Current Production Environment (CPE). IRDB serves as the protected and dedicated data authoritative repository for receiving and persisting validated 1094/1095 ACA Information Returns data for individuals, employers, and insurers. The data is required to provide support for the statutory obligations of the Patient Protection and Affordable Care Act (PPACA). IRDB accepts IR (Information Returns) and PBBA (Partnership Bipartisan Budget Act) data from the Correspondence Examination Automation Support (CEAS) system. IRDB supports two (2) key business capabilities of the IR ACA forms: (1) Receiving and Storing Validated Information Returns Data (Paper and Electronic). In support of the IR Receive and Store 1094/1095 ACA IR Data process area, IRDB receives and stores validated 1094/1095 Data (electronic) from ACA Information Returns (AIR) via the Enforcement Management Information System (EMIS). IRDB stores all electronically filed 1094/1095 Bs/Cs. IRDB stores all 1095A submissions, receive and store paper 1094B/C Fact of Filing Data from AIR through the EMIS. IRDB receives the PBBA form 8985/896 data from the CEAS system. The IR PBBA data consists of data from electronic PBBA 8985/8986 forms. IRDB stores the validated IR PBBA form data within the IRDB DB for future consideration of client use. (2) Providing access to the ACA Information Returns Data. In support of the Provide Access process areas, IRDB provides access to validated ACA IR Data for Fact of Filing through Analytics and Reporting (A&R). Current interfaces for the IR ACA data: a) An external interface to AIR with Interface Control Document (ICD) 157 - IRDB receives and stores IR data from AIR after AIR has performed validation checks. The IR data primarily consists of data from electronic 1095A forms, paper and electronic 1094/5 B forms and electronic 1094/5 C forms. b) A&R with ICD 158 - IRDB provides access to the IR Data for querying and reporting. c) Compliance Data Warehouse (CDW) with ICD 220 - The Oracle Data Pump Import utility. IRDB data is imported initially by the connected CDW Oracle database instance in the CDW staging area via database link. d) Integrated Production Model (IPM) with ICD 145 - IRDB to IPM interfaces is for all bulk transfers of ACA data from IRDB to IPM via ETL. Data is stored in IPM to support the need for ACA data analytics and reporting. e) IRPS with direct Java Database Connection (JDBC) - IRDB Stores Information Returns and provide access to IRPS to perform Data Certification processes. IRDB stores the indicators for the IRs after the Data Certification process is completed by IRPS. f) IR Entity Service with direct JDBC - IRDB supports IR Entity Service which provides the ability to access ACA Information Returns via Direct JDBC using Corporate Files On-Line (CFOL) Command Codes to respond to taxpayer and submitter inquiries. Current interface for the IR PBBA data: a) IRDB receives data through an external interface to CEAS defined by the Interface Control Document (ICD) PBBA-CEAS-IRDB-ICD-V1.1 and stores the IR PBBA data from CEAS. IRPS performs validation / certification checks of the IR PBBA data prior to CEAS transmitting the data to IRDB. There are no additional or planned external system interfaces and/or enhancements to external system interfaces for IRDB. There is no IRDB interface for viewing or altering the records stored in any IRDB schemas. All data contained in IRDB is maintained in its original state, with no change to the integrity or quality of the data. IRDB does not manipulate or

apply business rules to the data. There is no utilization of SBU data for testing, but rather synthetic data. Test data is generated through request and contains specifics to the type of request needed. This same type of synthetic test data is also utilized for integration testing under AIR and PBBA.

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)

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

Information Returns Database requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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 Information Returns Database requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number
Other Taxpayer 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
Phone Numbers
Date of Birth
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:

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.

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

Yes

Describe the other types of SBU/PII that are applicable to this system.

Date of Death

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

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.

Information Return Database (IRDB) is responsible for receiving Information Return (IR) Forms 1094/1095 A/B/C data from Information Returns (AIR), IR Form 8985/8986 data from Correspondence Examination Automation Support (CEAS) and making the data available to Fact of Filing, Reporting, and other consumer systems for use in administering the provisions of Information Returns. The SBU/PII elements listed in this PIA were determined to be the minimum information required for that purpose. IRDB does not have the ability to manipulate, change or delete any of the data elements contained within these files. Therefore, IRDB does not itself have a business need or use for the SBU/PII identified in this PCLIA, other than to receive it from one application and store it for use by other applications. This applies to all SBU/PII elements listed in this PCLIA. The SSN is used to identify a taxpayer on the ACA & PBBA Information Return forms.

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

The IR information/data transmitted by AIR and CEAS to IRDB will be assumed to be complete and correct.

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 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: ACA Information Systems (AIR)
Current PCLIA: Yes
Approval Date: 9/28/2020
SA&A: Yes
ATO/IATO Date: 6/17/2018

System Name: Correspondence Examination Automation Support (CEAS)
Current PCLIA: Yes
Approval Date: 2/18/2021
SA&A: Yes
ATO/IATO Date: 10/3/2019

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?

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?

Though this system does not notify individuals, the individual information utilized is received from a system that provides taxpayers with notice and rights to consent and/or amend, as needed, according to various IRCs, through notifications such as Publication 1. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

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

No

Why not?

Mandated by Federal Tax Regulations. The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information.

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

All data contained in IRDB is maintained in its original state, with no change to the integrity or quality of the data. IRDB does not manipulate or apply business rules to the data. All due process considerations for any system that uses data stored in IRDB are the responsibility of that system.

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 Only

System Administrators: Read Write

Developers: Read Only

IRS Contractor Employees

Contractor Users: Read Only

Contractor System Administrators: Read Write

Contractor Developers: Read Only

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

Database access is requested via an Online (OL) Form 5081. Access is granted on a need-to-know basis. The OL5081 enrollment process requires that an authorized manager approve access requests on a case by case basis. Access approval is based on the Users role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments; they are restricted from changing the boundaries of their access without management approval. The employee's access will be terminated once they no longer require access to the Database. Deletion from the active access role is also performed through the OL5081.

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.

Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6. The National Archives and Records Administration has approved the IRDB Retention Period for records retention to Delete/destroy data 3 years after cutoff. This is scheduled under DAA-0058-2016-0019. RCS 22, Item 56.

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?

4/29/2020

Describe the system's audit trail.

IRDB does not have an interface for online viewing or altering of individual records. System administrators do not create, read, update or delete individual IRDB data records as part of their normal responsibility. The IRDB audit process and audit trail is to: - Identify actionable events for each IRDB process or COTS product. These are events that either result in IRDB data being created, read, updated, or deleted, or that result in system administrators altering

or affecting the IRDB system environment. - For each actionable event, the appropriate auditable event is created that captures sufficient information to support later review or analysis of the event. The auditable event creates audit records that are first written to logs, using the capabilities provided by each COTS product or process. There is a large list of identified actionable and auditable events and they are documented in the Audit Plans of either the IRDB application or its supporting COTS products. For example, database level auditing is being performed by IBM Guardium. IBM Guardium applies the Oracle audit plan to the data it captures and passes that data to ArcSight. (Note: Security Audit and Analysis System (SAAS) auditing requirements have been deferred by Enterprise Security Audit Trails (ESAT) Program Management Office to a later release).

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

DocIT

Were all the Privacy Requirements successfully tested?

No

Please explain which Privacy Requirements were not tested and why?

IRDB is a machine-to-machine application that is not accessible to the public, thus limiting privacy issues. Privacy requirements were addressed during system design and are reviewed during each new PCLIA approval.

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Testing is in accordance with IAW 10.5.8 - Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments.

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?

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