Date of Approval: May 3, 2018 PIA ID Number: 3**355**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Information Returns Database, IRDB

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

AFFORDABLE CARE ACT (ACA) INFORMATION RETURNS DATABASE PIA#1553

Next, enter the **date** of the most recent PIA. 1/13/2016

Indicate which of the following changes occurred to require this update (check all that apply).

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

Were there other system changes not listed above? Yes

If yes, explain what changes were made. The PIA is approaching a 3-year anniversary. Renewal of current Privacy & Civil Liberties Impact Assessment. System is undergoing Security Assessment and Authorization.

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

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

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

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.

Affordable Care Act (ACA) Information Returns Database (IRDB) is a production system within the ACA program and is not considered part of the Current Production Environment (CPE). IRDB was developed independently within the ACA scope to support ACA and Non-ACA functionality. 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). The data stored on the IRDB is a subset of the ACA Information Returns Architecture to provide a centralized repository to receive and store validated 1094/1095 ACA Information Returns (IR) submissions and provide access to the IR data for Fact of Filing, Reporting, and other ACA and Non-ACA consumer systems. ACA IRDB supports two (2) key business capabilities (1) Receiving and Storing Validated Information Returns Data (Paper and Electronic). (2) Providing access to the ACA Information Returns Data. 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. 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). IRDB also provides access to validated ACA IR Data for Reporting and other ACA and Non-ACA consumer systems. Current interfaces; 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. Lastly, 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. 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. Due process is provided pursuant to 26 United States Code (USC).

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 Yes On Spouse Yes 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)
Yes Individual Taxpayer Identification Number (ITIN)
Yes 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 memorandum M-17-12 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 SSN's 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.

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

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
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
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

.

6d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Date Of Death

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
No	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? Yes

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.

IRDB is responsible for receiving Form 1094/1095 data from ACA Information Returns (AIR) and making the data available to Fact of Filing, Reporting, and other ACA consumer systems for use in administering the provisions of the ACA. 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 PIA, 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 PIA. The SSN is used to identify a taxpayer on the ACA Information Return forms.

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

Information/data coming from ACA Information Returns (AIR) will be assumed to be complete and correct.

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? Yes

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

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

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

SORNS Number	SORNS Name
Treasury/IRS 24.030	Customer Account Data Engine Individual Master File
Treasury/IRS 24.046	Customer Account Data Engine Business Master File
Treasury/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 PIA?	PIA Approval Date	SA & A?	Authorization Date
ACA Information Returns (AIR)	Yes	10/17/2016	Yes	05/19/2017

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? No

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?
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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If 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.

19. 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.

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-Only
Managers	No	
Sys. Administrators	Yes	Read and Write
Developers	Yes	Read-Only

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Moderate
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Read and Write	High
Contractor Developers	Yes	Read-Only	Moderate

21a. How is access to SBU/PII determined and by whom? Access to the Information Returns Database 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.

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? Yes

22a. 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.

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.

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)? In-process

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion? 9/1/2018

23.1 Describe in detail the system s audit trail. ACA 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).

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 9/1/2018

24.3 If **completed/ or in process,** 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.

K. SBU Data Use

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

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? No

If **yes,** provide the date the permission was granted.
If **no**, explain why not. Permission was granted per the requirements of the forms that were the predecessors for Forms 14664 and 14665. Permission per Forms 14664 and 14665 is in progress.

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: More than 1,000,000
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? No

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? No

End of Report