A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: December 15, 2014 PIA ID Number: **983**

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Affordable Care Act Information Returns Database, ACA/IRDB

2a. Has the name of the system changed? No

3. Identify how many individuals the system contains information on

Number of Employees:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	Over 1,000,000

4. Responsible Parties: N/A

5. General Business Purpose of System

ACA 5.0 Information Returns Database (IRDB) R1 is a new system within the ACA program and is not considered part of the Current Production Environment (CPE). IRDB was developed independently within the ACA 5.0 CDR R3 scope to support ACA functionality. IRDB serves as the protected and dedicated data 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 IRDB supports two (2) key business capabilities (1) Receiving and storing validated information returns data (paper and electronic), and (2) Providing access to the ACA Information Returns Data. IRDB will store all electronically filed 1094/1095 Bs/Cs. IRDB stores all 1095A submissions, and receives and stores paper 1094B/C Fact of Filing data from AIR through the Enterprise Informatica Platform (EIP). EIP is used for bulk (asynchronous) data exchanges between IRDB and IPM (SYS7) to extract ACA information returns data. There are two project system interfaces. AIR (SYS 12) provides validated 1094/1095 ACA Information Returns to IRDB via the EIP. Business Analytics (BA) queries IRDB data for reporting. There are no 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 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) No

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. none

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	Yes
Employees/Personnel/HR Systems	No
Other	No
Other Source	N/A

---

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Salary Information	Yes	No
Date of Death	Yes	No
Income Level	Yes	No

10a. What is the business purpose for collecting and using the SSN ?

The SSN is used to identify a taxpayer on the ACA Information Return forms.

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

http://www.irs.gov/pub/irs-wd/00-0075.pdf http://www.law.cornell.edu/uscode/text/26/6109 Section 7801 and 7803 of the Internal Revenue Code.

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

IRS and Congress have not provided for an alternative means to identify taxpayers.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

No strategy exists currently for the application.

Describe the PII available in the system referred to in question 10 above.

Taxpayer identification information and tax-related data required per ACA regulations.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

ACA 5.0 IRDB R1 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 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).

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: No

b. Other federal agency or agencies: Yes

If **Yes**, please list the agency (or agencies) below:

Federal Health Insurance Exchanges

c. State and local agency or agencies: Yes

If **Yes**, please list the agency (or agencies) below:

State Health Insurance Exchanges

d. Third party sources: Yes

If yes, the third party sources that were used are:

Possible third Party Health Insurance Exchanges.

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

IRDB will collect the minimum information required to administer the provisions of the ACA. IRDB serves as the protected and dedicated data repository for receiving and persisting validate Form 1094/1095 data ACA Information Returns data for individuals, employers, and insurers. The Project office will provide the PII listed above to allow the verification of ACA Information Returns (IR) submissions and access to the IR data for Fact of Filing, Reporting, and other ACA consumer systems.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	Yes
To provide taxpayer services	Yes
To collect demographic data	No
For employee purposes	No
Other:	No

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet? N/A

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? No

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

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.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

4053	Form 1094-B	Transmittal of Health Coverage Information Returns
4054	Form 1094-C	Transmittal of Employer-Provided Health Insurance Offer and Coverage Information Returns
4055	Form 1095-A	Health Insurance Marketplace Statement
4056	Form 1095-B	Health Coverage
4057	Form 1095-C	Employer-Provided Health Insurance Offer and Coverage

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		No Access
Managers		No Access
System Administrators		Read Write
Developers		No Access
Contractors:	Yes	
Contractor Users		No Access
Contractor System Administrators		Read Write
Contractor Developers		No Access
Other:	No	

If you answered yes to contractors, please answer **22a.** *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level"background investigation? Yes

23. How is access to the PII determined and by whom?

The Information Return Data will be available to the business via the Business Objects Environment. Access and Usage of the BOE is controlled and managed by each of the Business Operating Divisions based on the requirements of an individual's roles and responsibilities.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

Information Returns data coming from the various Health Insurance Exchanges via the ACA AIR project will be assumed to be complete and correct.

25. 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

25a. 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.

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.

The Affordable Care Act IRDB is unscheduled. The IRS Records and Information Management (RIM) Program Office has been notified of IRDB's status and will assist in drafting a request for records disposition authority (for submission to the National Archives) when data retention requirements are finalized. When approved by NARA, disposition instructions for IRDB system inputs, master files data, outputs, and system documentation will be published in IRS Document 12990, exact Records Control Schedule and item number to be determined.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
For data requests from other ACA applications (A2A), access to IRDB data is controlled by the use of secure certificates. Only authorized systems and Data Base Administrators (DBA) are allowed to access IRDB data, this is addressed through the audit plan.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

The IRDB will be located within the IRS network, and is protected, by its positioning with other ACA applications, IRDB uses EIP for data exchanges between other systems and IPM – SYS7 will access IRDB to extract Information Returns Data. IRDB does not have an online interface for viewing Data at rest (i.e., individual data records). For data at rest, access is only granted to IRS employees with specific permission, i.e., System Administrators (SA) or DBAs. Data in flight and data in transition are also referred to as data in motion. Data in motion for ETL (i.e, data loads to IPM) is protected by the mechanisms and design of the ETL process. The ETL process is a sequence of automated jobs, programs and processes. System administrators managing the ETL process monitor the sequence for completion, but in general do not need to access specific IRDB data records during the process. BOE access to the Information Return Data is managed and controlled by the Business Operating Divisions based on individual roles and responsibility.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

Vulnerability scans will be run monthly to monitor/detect known and unknown threats and vulnerabilities.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*? No

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

No SORN Records found.

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No