Date of Approval: October 31, 2018 PIA ID Number: **3736**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. System 7.3 ACA Data Mart, Sys 7.3 ACA Data Mart

2. Is this a new system? No

2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

System 7.3 Affordable Care Act (ACA) Data Mart, Sys 7.3 ACA Data Mart, 1495, MS4B

Enter the approval **date** of the most recent PCLIA. 01/13/2016

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

Yes Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
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
No Expiring PCLIA

Were there other system changes not listed above? No

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

Application Development (AD) Data Delivery Services (DDS) Governance Board (GB)- AD: DDS:GB. NOTE: Information Sharing and Reporting-Analytics & Reporting (ISR-A&R) was recently moved to Wage & Investment (W&I), however, we are still working with the AD: DDS:GB for our 2018 Milestone Exit Review (MER) and have not yet been assigned to a W&I GB.

3.a. Check the current Enterprise Life Cycle (ELC) 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? No

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.
Data Analytics supports the Internal Revenue Service (IRS) legislatively-mandated implementation of ACA, the Information Technology (IT) and Application Development (AD) goals. Data Analytics primary focus is to support the ACA. Data Analytics includes analyzing and performing statistical or business operational reporting on the taxpayer, marketplace, issuer, employer, and waiver / extension requestor related data. For optimized reporting and analysis, ACA information will be collected from various sources and organized into System 7.3 - ACA Data Mart.

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

6.a. 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 all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
No	Interfaces with external entities that require the SSN
Yes	Legal/statutory basis (e.g. where collection is expressly required by statute)
No	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

SSNs are provisioned for Business Units (BU) access to accomplish their compliance related activities.

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. System 7.3 ACA Data Mart 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.

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

If **yes**, specify the information.

Selected	PII Element
Yes	Name
Yes	Mailing address
No	Phone Numbers
No	E-mail Address
Yes	Date of Birth
No	Place of Birth
No	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
No	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	Proprietary data	Business information that does not belong to the IRS
Yes	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. 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.

Document Locator Number, Transmitter Control Code and Individual Date of Death.

6.e. 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

6.f. 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.

The SSN is used to evaluate and determine shared responsibility payment related to Premium Tax Credit. The date of birth, date of death, mailing address and individual name are used to establish identity when an SSN is not provided. The EIN is used to evaluate employers and establish whether they have met their responsibility for providing medical coverage to individuals employed by them.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

The information is received from internal IRS systems which contain internal consistency checks. The information has been validated for accuracy by the system sending the data and has been deemed reliable.

C. 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.

9. 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

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

SORNS Number	SORNS Name
IRS 42.021	Compliance Programs and Project Files
IRS 34.037	Audit Trail and Security Records System

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

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

11.a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
ACA Compliance Validation (ACV) Correlation	Yes	01/26/2016	Yes	09/09/2015
Integrated Production Model IPM R10.0	Yes	10/27/2017	Yes	04/01/2015

11.b. Does the system receive SBU/PII from other federal agency or agencies? No

11.c. Does the system receive SBU/PII from State or local agencies? No

11.d. Does the system receive SBU/PII from other sources? No

11.e. Does the system receive SBU/PII from **Taxpayer** forms? No

11.f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. DISSEMINATION OF PII

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, Radio Frequency Identification (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 (or is) notice provided to the individual prior to collection of information? Yes

17.a. 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?
This system does not collect any information directly from taxpayers. PII information is received from the Integrated Production Model (IPM), and the ACA Compliance Validation (ACV) Correlation whose information comes from the submission of tax returns submitted directly to the IRS through other internal IRS systems. 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

18.b. If individuals do not have the opportunity to give consent, why not?
Information is received downstream and used for analysis purposes only. 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?
Publication 1 “Your Rights as a Taxpayer” explains the rights of the taxpayer, which includes the right to challenge the IRS’ position and be heard; and the right to appeal an IRS decision in an independent forum.

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	Yes	Read-Only
Sys. Administrators	Yes	Administrator
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	Low
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Read-Only	Low
Contractor Developers	Yes	Read-Only	Low

21.a. How is access to SBU/PII determined and by whom? Access to the System 7.3 ACA Data Mart 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.

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

22.a. 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.

Sys 7.3 can be covered under Doc.12829, The General Records Schedule 4.3, item 020 because it is relying on extracted data from other repositories. Several of the data supplying repositories are scheduled; Individual Master File (IMF) (RCS 29, Item 203), Business Master File (BMF) (RCS 29, Item 201), Payer Master File (PMF) (RCS 19, Item 64a). One of the data supplying repositories is unscheduled, Coverage Data Repository (CDR). The IRS Records and Information Management (RIM) Program Office will work with the system owner of CDR on a request for records disposition authority. When approved by National Archives and Records Administration (NARA), disposition instructions for CDR inputs, system data, outputs, and system documentation will be published within the Internal Revenue Manual (IRM) or as part of the Records Control Schedule. When finalized, the Business Unit is proposing to retain data in Business Analytics (BA) as per business requirement: Information Returns Database (IRDB) six years, IMF/BMF/Individual Return Transaction File (IRTF) three years, PMF six years, CDR three years.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? No

23.c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1. Describe in detail the system's audit trail. Audit capabilities are inherited from the underlying infrastructure components such as Enterprise Business Intelligence Platform (Business Objects and Tableau), BDA, and Enterprise Informatica Platform BDA.

J. PRIVACY TESTING

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

24.a. If **yes**, If yes, was the test plan completed? Yes

24.a.1. If **yes**, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? The test results are stored on a IRS SharePoint site collection.

24.a.2. If **yes**, were all the Privacy Requirements successfully tested? Yes

24.a.3. If **yes**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? ISR-A&R, like other IRS systems, has to conduct a series of tests to validate the system configuration. Data accuracy is not only a requirement of the IRS principles; it is part of the Privacy Act and Federal Taxpayer Information protection laws and regulations. In order to protect taxpayer information, the recommendation is to use sanitized data when possible in order to reduce the risk of PII being seen by individuals without a need-to-know and creating an incident. The IRS has established Internal Revenue Manual (IRM) 10.8.8.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26.a. IRS Employees:	Not Applicable
26.b. Contractors:	Not Applicable
26.c. Members of the Public:	More than 1,000,000
26.d. 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 Recommendations of the 9/11 Commission 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

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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