Date of Approval: **September 27, 2019**

PIA ID Number: **4395**

## SYSTEM DESCRIPTION

*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

*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?*

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

*What is the approval date of the most recent PCLIA?*

10/31/2018

*Changes that occurred to require this update:*

Addition of Personally Identifiable Information (PII)

*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.*

Application Development (AD) Data Delivery Services (DDS) Governance Board (GB)-AD:DDS:GB

*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?*

No

## 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.*

Data Analytics supports the Internal Revenue Service (IRS) legislatively-mandated implementation of the Affordable Care Act (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.

## 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)*

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 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. 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.

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

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 (SBU List)*

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

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

*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.*

Document Locator Number, Transmitter Control Code and Individual 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.*

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.

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

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.

## 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

IRS 34.037 Audit Trail and Security Records System

## RESPONSIBLE PARTIES

*Identify the individuals for the following system roles:*

## For 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 Compliance Validation (ACV) Correlation

Current PCLIA: Yes

Approval Date: 6/25/2019

SA&A: Yes

ATO/IATO Date: 9/9/2015

System Name: Integrated Production Model IPM R10.0

Current PCLIA: Yes

Approval Date: 10/27/2017

SA&A: Yes

ATO/IATO Date: 6/6/2019

*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?*

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.

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

No

*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.

*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.

## 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

Managers: Read Only

System Administrators: Administrator

*IRS Contractor Employees*

Contractor Users: Read Only

Contractor System Administrators: Read Only

Contractor Developers: Read Only

*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.

## RECORDS SCHEDULE

*Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) archivist 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.*

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.

## SA&A OR ASCA

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

No

*Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?*

Yes

*Describe the system's audit trail.*

Audit capabilities are inherited from the underlying infrastructure components such as Enterprise Business Intelligence Platform (Business Objects and Tableau), Big Data Analytics (BDA), and Enterprise Informatica Platform BDA.

## 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)?*

The test results are stored on an IRS SharePoint site collection.

*Were all the Privacy Requirements successfully tested?*

Yes

*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?*

Information Sharing Reporting - Analytics & Reporting 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.

## 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