NOTE: The following reflects the information entered in the PIAMS website.

Date of Approval: August 18, 2015 PIA ID Number: **1392**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Affordable Care Act (ACA) 6.1, Coverage Data Repository (CDR) R4.0, CDR

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) 5.0 MS 4B, Coverage Data Repository (CDR) R3

Next, enter the **date** of the most recent PIA. 12/5/2014

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? No

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
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	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.

In ACA 3.0 Coverage Data Repository (CDR) R1 the CDR application maintains a data repository that provides the operational database for other Affordable Care Act (ACA) applications. ACA applications, specifically Information Sharing and Reporting (IS&R), provide data to applicants when purchasing health insurance through an Exchange. This data is required for the statutory obligations of the Patient Protection and Affordable Care Act (PPACA). The data stored on the CDR is a subset of data maintained by the Integration Production Model (IPM). The IPM system contains tax return data captured from taxpayers and taxpayer-submitted IRS forms. A key business process supported by the CDR Repository is providing income and family size information. In order to receive Advance Premium Tax Credit an applicant must enroll through the Federal or State-based Exchange. During the enrollment process, an applicant may request financial assistance. If so, the Exchange requests income information, on behalf of the applicant, via the Center for Medicare and Medicaid Services (CMS) Data Services Hub. The CMS Hub forwards the request to the IRS Portal. The specific data provided to the applicant is the result of the Income and Family Size Verification (IFSV) calculation. The actual calculation is made by the ISFV application using tax-related data provided, upon IFSV request, by CDR. CDR does not have an interface for online viewing or altering of individual data records. System administrator access to CDR is through two Commercial-Off-The-Shelf (COTS) products: Oracle (for supporting the repository itself) and Informatica (for supporting the CDR data load process). System administrators do not create, read, update or delete individual CDR data records as part of their normal responsibility. All data contained in CDR is maintained in its original state, with no change to the integrity or quality of the data. CDR does not manipulate or apply business rules to the data. Where taxpayer information is shared, all security and privacy requirements are adhered to and maintained by the CMS Data Services Hub. In ACA 4.0 CDR R2, CDR R2 was developed to receive and store the monthly Exchange Periodic Data (EPD) submissions from the Health Insurance Exchanges (HIE) through the CMS Data Services Hub. The EPD data is the month by month submission of information of individuals who purchased coverage through the HIEs and is needed by the IRS to accurately perform tax administration. The validated data is received from IS&R using the Enterprise Informatica Platform (EIP). The data is stored initially in a Staging Schema and then transformed into the Exchange Schema for access in future releases. The EPD is also transformed into the Reporting Schema to support Reporting using the Business Objects Environment (BOE). The EPD being received and stored in ACA 4.0 CDR R2 includes Household Coverage data, Individual Coverage data, Individual and Employer Entity and Relationship data, Advanced Premium Tax Credit (APTC) payment data, Exemption Data, Small Business Health Options Program (SHOP) Employer data, and SHOP Employee data. Consistency checks are run by IS&R on all data before being written in CDR. There are no CDR interface for viewing or altering the records stored in any of the three schemas. In ACA 4.0 CDR R2 like ACA 3.0 CDR; all data contained in CDR is maintained in its original state, with no change to the integrity or quality of the data. CDR does not manipulate or apply business rules to the data. This data is provided to downstream systems to support tax administration and statistical analysis. In addition, the information is used to support statistical analysis by the Office of Research Analysis and Statistics (RAS) which will use this data to estimate various statistics, such as the counts and amounts of the APTC that have been claimed, as well as other aggregate statistics on certain characteristics of ACA Health Insurance Exchange participants. In ACA 5.0 CDR R3, CDR extended prior release functionality to support At-Filing Compliance and Customer Service (CS) functional process areas. In support of the At-Filing Compliance process area; CDR will provide EPD and Static Reference Data to the ACA Verification System (AVS) for At-Filing examination. CDR stores Static Reference Data to support ACA Processes. In support of the Customer Service process areas, CDR was modified to provide EPD and Static Reference Data to CS/AMS. In support of analytics and reporting, modifications were made to CDR to receive and store Income and Family Size Verification (IFSV) Response Code Data. In this update, ACA 6.1 CDR 4.0 purpose is to retrieve, store and provide the information to help ensure that taxpayers receive the appropriate amount of PTC Advance Payments of the Premium Tax Credit (APTC) or make the appropriate Shared

Responsibility Payment (SRP). ACA 6.1 CDR R4 extends the functionality implemented in ACA 3.0 CDR R1, which supports the Income and Family Size calculator, to include the APTC Failure to Reconcile data. This will be accomplished through existing interfaces with no changes to how data is transported or stored. Due process is provided pursuant to 26 USC. There is no CDR interface for viewing or altering the records stored in any CDR schemas. All data contained in CDR is maintained in its original state, with no change to the integrity or quality of the data. CDR does not manipulate or apply business rules to the data.

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 No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
No	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	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).

No alternative exists currently for the application. This program is aware of and part of the IRS-wide SSN elimination and reduction program.

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
No	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
No	Tax Account Information	No	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. PII Name On Public? On Employee? Salary Information Yes No Date Of Death Yes No Income Level Yes No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

No	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.

The SSN is used to provide tax return data to the Income and Family Size Verification process.

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 IPM will be assumed to be complete and correct. Exchange Periodic Data is validated by the ACA Information Sharing (IS) project according to rules agreed to with the ACA Business team and their Center for Medicare and Medicaid Services (CMS) counterparts.

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 **other,** explain your answer**.**

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

SORNS Number	SORNS Name
Treas/irs 24.030	CADE Individual Master File (IMF)--Treasury/IRS
Treas/IRS 24.046	BMF
Treas/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. N/A

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
Integrated Production Model (IPM)	Yes	03/12/2014	Yes	08/02/2011

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If **yes**, for each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Health and Human Services	Encrypted MTOM XML	Yes
Center for Medicare and Medicaid Services	Files	No

11c. Does the system receive SBU/PII from State or local agency (-ies)? 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, cloud, 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?
The collection of tax information from individuals is provided for by the Federal Tax Regulation and provided to use by the Affordable Care Act processes by the Patient Protection and Affordable Care Act.

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.

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

All data contained in CDR is maintained in its original state, with no change to the integrity or quality of the data. CDR does not manipulate or apply business rules to the data. All due process considerations for any system that uses data stored in CDR 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	No	
Managers	No	
Sys. Administrators	Yes	Read and Write
Developers	No	

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? Starting with CDR R2 the business is able to generate reports about the Exchange Periodic Data (EPD) using Business Objects Exchange (BOE). 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. In CDR R3, the Exchange Periodic Data will be made available to the AMS system to be used by Customer Service representatives and Tax Examiners. Their access is controlled via a negative TIN check performed by IS&R before presenting the request to CDR.

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? No

22b. 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 Coverage Data Repository (CDR) is unscheduled. CDR was deployed in October, 2013 and maintains a recordkeeping repository of data relating to Affordable Care Act projects. The IRS Records and Information Management (RIM) Program Office has been notified of CDR'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 CDR 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.

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)? Yes

23a. If **yes**, what date was it completed? 4/23/2015

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

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?
CDR was tested to ensure that only authorized system to system access is performed with proper authentication using Siteminder Tokens.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Detailed test cases and results are stored in the Requisite Quality Manager repository.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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? Yes

If **yes,** provide the date the permission was granted. 8/1/2014

25b. **If yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy? Yes

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