Date of Submission: November 6, 2015 PIA ID Number: **1472**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Customer Account Data Engine 2, CADE 2

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.

Customer Account Data Engine 2, CADE 2

Next, enter the **date** of the most recent PIA. 6/24/2015

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
Yes	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. Modifications were made to the system components that required an updated security assessment which automatically triggers the need for an updated PCLIA.

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.

The IRS Individual Master File (IMF) is currently the IRS authoritative data source (ADS) for individual tax account data. This means that IMF is the system that other IRS systems currently rely on for individual tax account data necessary for tax administration. CADE 2 will eventually replace IMF as the ADS for individual tax account data, providing information feeds to other IRS internal systems so they can process tax returns. One such application is the Integrated Data Retrieval System (IDRS) where active tax cases are handled. To accomplish this, CADE 2 contains all individual taxpayer account information in a relational database which is designed to recognize relationships between the information in order to improve the speed at which refunds are processed. Using key fields and linking data tables together allows the data to be located quicker and thus improving processing times. Along with the improved times, CADE 2 allows IRS frontline employees to view more accurate and timely account information due to modifications that will update information in the system more frequently, on a daily verses a weekly basis. This allows CADE 2 to ensure accuracy, completeness, and enhanced availability of information for IRS employees who rely on this information to process refunds and improves services to taxpayers by allowing refunds to be processed faster and with greater accuracy. CADE 2 will also continue to evolve and improve its existing capabilities to ensure data integrity is not compromised. To achieve this CADE 2 is implementing further enhancements through smaller projects to address the changes that are expected to take place during the continual transition from IMF. This includes issues like the potential for irregularities in data formats, as well as, providing data and reports to other IRS databases (such as the Integrated Production Model (IPM) within Big Data Analytics (BDA)) and applications or business offices requiring access to taxpayer data or transcripts. One such CADE 2 project is the Database Conversion (DBC) process in which IMF Annual and Mid-Year Conversion changes are applied to the CADE 2 database while retaining CADE 2 historical data (changes to transactions, tax modules, balances, tax return records, taxpayer records, and pending events). Another ongoing effort is the Production Support Environment (PSE) used for break-fixes and data validation to ensure accuracy and code validation.

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)
Yes 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 SSN is the primary means of querying the database. It is the only unique identifier associated with taxpayers, spouses, and dependents that can be used to ensure the correct

record is accessed by older IRS systems. CADE 2 continues to examine all new requests that state a need to access the SSN to ensure there is a specific requirement and business approval to access the SSN in order to perform official IRS functions. Prior to any future connections to downstream systems the IRS shall examine alternative solutions and will work with system owners to try and mitigate the need for the SSN. In addition, IRS will annually review CADE 2 SSN uses and continue to find ways to replace, mask, or truncate the SSN. In addition, IRS is undertaking efforts to expand the use of a modified system identifier, Document Locator Number (DLN), or a truncation of the SSN. A plan is reviewed annually examining reports, system connections, and requests that use the SSN in order to determine if an alternative can be used.

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
Yes	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
Yes	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	Yes	Yes

6c. 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 which if improperly used or disclosed could

	Information	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.

6d. Are there other types of SBU/PII used in the system? No

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.

The Personally Identifiable Information (PII) collected from the IRS 1040, 1040A, 1040X, and all supplemental documentation filed along with an individual's tax information is used to validate an individual's taxes. The only SBU/PII data CADE 2 uses is that which is necessary to assess the taxes. This includes the SSN since it is the one unique identifier that taxpayers have to identify themselves.

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

With CADE 2 running daily updates the database is able to validate and ensure data completeness by assessing the data format and flagging errors that could affect a tax return assessment. A mainframe application validates data through a series of applied business rules. During this processing, if any data elements are determined to be outside of the expected formatting parameters, the element is flagged for further analysis by the system. If the system is unable to correct the element, a ticket is created and the element will be examined by appropriate personnel that can resolve the issue. In the future, CADE 2 will verify the accuracy of SSNs against Social Security records through another IRS application. Taxpayer information will continue to be processed by using IMF until CADE 2 is officially accepted by both the Chief Financial Officer and Government Accountability Office (GAO) as the authoritative data source for individual tax account data. In addition, when other internal systems that rely on CADE 2 data discover inaccurate or incomplete information due to their direct interaction with individual taxpayer, the information is resubmitted through appropriate processes and the taxpayer information is updated.

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
24.030	CADE Individual Master File
24.046	CADE Business Master File
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 Data Retrieval System (IDRS)	Yes	08/03/2014	Yes	03/08/2010
Individual Master File (IMF)	Yes	05/02/2014	Yes	05/02/2014

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 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? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Integrated Data Retrieval System (IDRS)	Yes	08/03/2014	Yes	03/08/2010
Big Data Analytics (BDA)	Yes	09/19/2014	Yes	11/26/2012
Integrated Production Model (IPM)	Yes	10/15/2014	Yes	07/14/2014

Identify the authority and for what purpose? The authority for processing taxpayer information is 5 U.S.C. 301 and 26 U.S.C. 7801. The purpose for sharing taxpayer information received by other IRS systems and processed by CADE 2 is to assess and distribute tax returns. Information from CADE 2 is shared with IDRS for the purpose of providing data for open cases and shared with BDA and IPM for the purpose of providing data for a new data store that will address downstream system data requirements. CADE 2 is only a repository for taxpayer data and it does not interact directly with taxpayers like other systems regarding return transactions and authorized taxpayer representatives

12b . Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? 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?
Notice is provided to individuals by other IRS applications or through forms (e.g., 1040 forms) that interact directly with the taxpayer at the time of collection. Due Process is provided pursuant to 5 USC.

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
CADE 2 does not collect any information directly from taxpayers. All information that is maintained by CADE 2 comes from the submission of 1040 forms submitted directly to the IRS through other IRS systems. Information from the 1040 form is collected and stored in IMF and is then subsequently shared with CADE 2. In the future, when CADE 2 is accepted as the ADS data will be sent directly to the CADE 2 DB. The 1040 form provides taxpayers information regarding the opportunity to decline or consent to providing the information. Due Process is provided pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?
CADE 2 is only a repository of taxpayer information submitted directly to the IRS through other IRS applications. CADE 2 does not interact with taxpayers directly and thus "due process" is addressed by other IRS applications that directly interact with taxpayers. Any issues that are identified by these other means will submit changes to CADE 2 through automated methods so an auditable record may be maintained. Due Process is provided to 5 USC.

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	Administrator
Developers	Yes	Read And Write

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? All contractors and employees must go through the Public Trust Clearance process before access is considered. Once cleared, an IRS employee or contractor must complete the proper request forms before access to CADE 2 is obtained. All access must be approved by the user's manager who reviews the access request form at the time of submission and on an annually basis. The system administrators/approvers will also verify group membership to ensure system rights are limited based on the employee or contractor's need-to-know in order to perform their official duties. For access to an environment where a new or modified system is being tested (i.e., a non-production supporting environment) users must complete the necessary SBU data training, complete an access request form, and in some cases as outlined by the requirements set forth within the Internal Revenue Manual (IRM), submit an elevated access letter that is approved by the Associate Chief Information Officer prior to granting access.

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.

CADE 2 development records continue to follow RCS (Document 12990) Information Technology Schedule 17. As for production records, a request for records disposition authority for the CADE 2 and its associated records is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by NARA, disposition instructions for CADE 2 inputs, system data,

outputs, and system documentation will be published within the IRM or as part of the Records Control Schedule. The expectation is that for the Enterprise Computing Center - Martinsburg, will continue to follow IRM 2.7.9. Smaller files and documents that fall outside the schedule are addressed by the project and kept only as long as necessary in order to perform their task.

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? 4/21/2015

23.1 Describe in detail the system s audit trail. The SA&A controls are assessed annually in accordance with the Annual Security Control Assessment (ASCA) to ensure system security and privacy compliance. Vulnerability scans and policy checkers are routinely run and if a vulnerability is detected efforts are made to address the concern upon discovery. In addition, CADE 2 development areas that utilize live data periodically review staff lists to ensure listed support personnel require the level of access requested.

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? 12/31/2015

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?
The CADE 2 system is going through a continuous System Test Plan due to its ongoing enhancements. Each enhancement has a different set of design requirements which includes security and privacy requirements that are assessed. The overarching privacy requirements are further defined into testable requirements that are reviewed by the development team. The identified requirements will then be tested and documented. Any risks that are discovered are reviewed and addressed. All this is being coordinated by Requirements Engineering Program Office and Cybersecurity and tracked in the Rational Requirements Tool and developer security assessment testing.

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. 3/31/2015

.

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