A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Common Data Processing Framework, CDPF

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.

      Data Services Framework, DSF, 1432, Development

      Next, enter the **date** of the most recent PIA.   6/27/2016

      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? No

      If yes, explain what changes were made.

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
Yes	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
Yes	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.

The Common Data Processing Framework (CDPF), also known as the Data Distribution Framework (DDF) or formerly known as the Data Services Framework (DSF), establishes a standard framework using modernized technical components to provide Customer Account Data Engine (CADE) 2 individual taxpayer data to downstream IRS systems and business units via the common data distribution service in the form of reports and files. In addition, some of the data created by the framework will be sent back to CADE 2 for historical and auditing purposes. To protect these transfers, Interface Control Documents are created describing the interface controls and security and privacy requirements. The framework will consist of custom Java code that will select data, transform it and generate an output. The outputs produced by this framework must adhere to the receiving systems capabilities and thus meet legacy and modernized data formats. To accomplish this, an environment, separate from the databases, was and continues to be developed. There are several projects that will be part of this CDPF boundary. Each project will create the specifics necessary to generate their required business report or taxpayer transcripts, duplicating the function already performed by the Individual Master File (IMF). The current IMF operation will retire following the development of this project. These projects will be implemented over time and will exit the various Enterprise Life Cycle (ELC) Milestones at different timeframes, depending on their development and implementation schedule. The reports will not be shared with the intended downstream system until later in their development lifecycle, after running in parallel with the production reports to allow for a comparison with the files generated by the IMF in order to assess accuracy. The different projects include Refunds which establishes a new interface from the CADE 2 database to IMF post-settlement runs. Chief Financial Officer (CFO) Critical Reports (CCR) which creates downstream CFO report interfaces leveraging data provided by CADE 2. The Authoritative Data Source (ADS) Transcripts will recreate a select set of transcripts that leverages the CADE 2 Database in order for CADE 2 to become the "Authoritative Data Source." Feed to IDRS (Integrated Data Retrieval System) establishes two interfaces between CADE 2 and IDRS. The first creates the daily extract file to send individual taxpayer accounts to IDRS. The second supports the request/response interface to send individual taxpayer accounts to IDRS. Unpaid Assessment (UA) is a smaller project that is separate from the larger UA project. It prepares revenue and refund statement requests used by the IRS as part of the custodial financial statement developed for the Government Accounting Office (GAO) financial audits. The Pending Payment Transaction (PPT) project will help to improve the accuracy of the financial reports by including the pending payment transactions in the unpaid assessment balance. The Individual Tax Processing Engine (ITPE) will update IMF processes that currently use an older assembly language with Java code. It will be the Data Services Framework project that will provide the common framework used by all these projects in the generation of reports and files. To accomplish this, projects will continue to use existing development environments and utilize prototype environments (some found offsite). The prototypes are examined from both a security and privacy perspective to ensure the data is protected. In some instances, synthetic, or made up data, will be used in order to reduce risk. This includes any offsite testing that may take occur. The CDPF also encompasses the Change Data Capture (CDC) Tool which provides a means to capture CADE 2 database changes and in order to update the CADE 2 Operational Data Store (ODS) Database schema on IPM/BDA. Finally, due to the complexity of some projects and their designs it should be noted that some IRS components outside of the CDPF boundary may be utilized. These components will still be assessed and tested to validate security and privacy requirements. Lastly, the development of these projects will utilize live data of which the appropriate compliance is met and documented.

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.)? <u>Yes</u>

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes   On Primary   Yes   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)
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).

<u>There are no plans to mitigate or eliminate all the uses of the SSN, at this time. The projects must first reproduce the exact IMF reports, transcripts, and files in order to authenticate and verify the accuracy of the outputs which will lead to accepting CADE 2 as the authoritative data source and replacing IMF. Second, it is important that feeds continue to reach downstream legacy systems that do not have the ability to use SSN alternatives. Even though an alternative is not used immediately the use of the SSN will continue to be assessed regularly to determine when the SSN usage may be mitigated or eliminated. Until such time, the SSNs are used within this system in accordance with Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.</u>

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc) <u>Yes</u>

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
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
Yes	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	No

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	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.

.

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.   The other types of SBU/PII data applicable to the system is that which is linked or linkable such as Tax Return and Financial Information which includes tax periods, penalty amount, interest amount, transaction code, transaction amount, assessed module balance, posted financial transaction, and disbursement.

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) is collected from the IRS 1040, 1040A, 1040X, and all supplemental documentation filed along with an individual's tax information which is processed by CADE 2 and then extracted by the framework or project. The SBU/PII data used within the security boundary is necessary to reproduce current IMF reports, transactions, and files used throughout the IRS by older legacy downstream systems and service centers. This includes the SSN since it is the one unique identifier that can be used to link taxpayer accounts to downstream legacy systems, address long term account analysis, and allow the comparison to current IMF outputs which strictly uses the SSN.

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

From a processing standpoint, the data used within the security boundary is validated after it is transferred to ensure completeness and accuracy from the taxpayer database. While the outputs created by the system are compared to the reports produced in IMF to verify accounting accuracy and completeness, as IMF is currently the authoritative data source and has produced the reports since their initial development. It is this verification which will help to validate the CADE 2 processes and allow CADE 2 to become the authoritative database. The reports will not be shared initially with downstream systems or IRS offices until the outputs are reproduced exactly as they are today.

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. # # Official Use Only

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	Yes	08/03/2014	Yes	12/19/2011
Customer Account Data Engine 2	Yes	11/06/2015	Yes	06/29/2015
Individual Master File (IMF)	Yes	03/06/2017	Yes	12/09/2016

    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
Enterprise Informatica Platform (EIP)	Yes	05/30/2013	Yes	05/21/2015
Redesign Revenue Accounting Control System	Yes	05/05/2016	Yes	08/12/2015
Custodial Detail Database (CDDB)	Yes	10/09/2014	Yes	06/29/2015
Customer Account Data Engine 2	Yes	11/06/2015	Yes	06/29/2015
Integrated Data Retrieval System	Yes	08/03/2014	Yes	12/19/2011
Individual Master File (IMF)	Yes	03/06/2017	Yes	12/09/2016

    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 is for processing, reporting, and sharing of tax return information that was received and processed by other internal IRS systems in order to

pass it along to downstream IRS businesses and applications that evaluate the processed data. The projects within the CDPF boundary supports CADE 2 as it works to enhance runs currently performed by IMF by replacing older code with a modern language which is more flexible and easier to manage.

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 where Due Process is provided pursuant to 5 USC. The project extract data from existing IRS databases and is several systems removed from the data collection.

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):
No information used within the CDPF security boundary is collected directly from taxpayers. All information that is processed by CDPF comes from tax information collected through tax forms or other applications that interact with taxpayers. It is at the time of collection that individuals have the opportunity to decline or provide consent. 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?
The components of the CDPF boundary support functions of IDRS and CADE 2 which is only a repository of taxpayer information submitted directly to the IRS through other IRS applications. The

projects do not interact with taxpayers directly and thus "due process" is addressed by other IRS applications that directly interact with taxpayers pursuant to 5 USC. Any issues that are identified by these other applications will work through the enterprise and submit changes through automated methods so an auditable record may be maintained.

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	
Developers	Yes	Administrator

Contractor Employees? Yes

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

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, access to projects within the CDPF boundary is obtained through the On-Line 5081 (OL5081) process. All access must be approved via the OL5081 system by the user's manager who reviews the access request at the time of submission and on an annual basis in order to verify the request and if the user has a need-to-know. 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 non-production supporting environments users must complete the necessary SBU (live) data training, request access through the OL5081, and in some cases as outlined by the requirements set forth within the IRM submit an elevated access letter that is approved by the Associate Chief Information Officer (ACIO) prior to granting access. The non-production environment will also routinely review access lists and verify accounts, removing ones that are no longer necessary. Every individual is reminded of their Unauthorized Access (UNAX) requirements where they are restricted to see certain taxpayer data and in many instance a third party tool is implemented to restrict access to that data.

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.

   Development records for all projects continue to follow RCS (Document 12990) Information Technology Schedule 17. As for output records, a request for records disposition authority for the various files 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 & IMF 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 RCS 19. 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. To ensure this compliance is met an automated process has been established to delete expired files in order to reduce the risk of storing them longer than necessary.

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)?   In-process

   23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion?   12/31/2016

   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. If a vulnerability is detected efforts are made to address the concern upon discovery. As each project kicks off an audit plan is reviewed and documented for each CDPF project. In addition, project development areas that utilize SBU (live) data periodically review staff lists to ensure listed support personnel still require access and have the appropriate level of access.

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? 12/1/2018

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 projects within the CDPF security boundary will go through a continuous System Test Plan due to ongoing development and project framework consolidation. Each individual project under the larger CDPF boundary has different scope and design requirements which are assessed against the privacy requirements. To accomplish this, each project not only addresses the overarching Privacy Requirements but will break down the requirements to decomposed requirements that are reviewed, implemented, tested, and documented to ensure appropriate action was taken to address them. All this is being coordinated by the Requirement Engineering Program Office (REPO) and Cybersecurity and tracked in the Rational Requirements Tool and developer security and privacy (formerly SA-11) 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.   4/23/2017

    25b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? 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?

Yes

    If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. This project is updating the process for generating reports, transcripts, and files that are already used by other IRS systems

and business units. In some cases, these generated documents may be specific in nature in order to address both tax and legal concerns and issues. The creation of these reports will be monitored and limited through the system or business requesting the information. The reports will also be carefully examined to ensure they are like in kind to the reports, transcripts and files currently produced. The projects will work closely with the existing report and data processes to ensure nothing new is added without first obtaining the necessary approvals.

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