Date of Approval: February 12, 2019 PIA ID Number: **3676**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Rational Collaborative Lifecycle Management, Rational CLM

2. Is this a new system? No

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

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

Rational tools initiative (RTI).

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.
Rational Collaborative Lifecycle Management (CLM) is an International Business Machine (IBM) lifecycle development solution designed to help manage the flow of people, process, and information. CLM consists of three separate components that integrate with each other: Rational Quality Manager (RQM), Rational Team Concert (RTC) and Doors Next Generation (DNG). The Rational CLM solution addresses the traceability requirements. Sensitive but unclassified (SBU) Data housed in the CLM repositories will be used by specified test teams to conduct acceptability testing on Internal Revenue Service (IRS) tax system software.

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
No	Legal/statutory basis (e.g. where collection is expressly required by statute)
Yes	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.

Without Master File data (SSNs) to conduct acceptability testing, the Enterprise System Testing organization cannot validate the software used to run the tax system. Because of this critical need, use of SSNs have been authorized by the Associate Chief Information Officer (ACIO).

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. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The Rational Collaborative Life Cycle Management requires the use of SSN's because currently there is no other identifier that can be used to uniquely identify a taxpayer. SSNs are permissible from the 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
No	Name
Yes	Mailing address
No	Phone Numbers
No	E-mail Address
No	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
Yes	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
No	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.
Yes	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
No	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? No

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.

Live data, which consist of SSNs, Mailing Address, Bank Routing Numbers, and Tax Account Information, is needed to provide a reliable testing effort. Without accurate data to conduct testing we cannot validate the software used to run the tax system. We have limited the use of live data only to what is relevant. Only CLM users that are on a live data waiver (LDW) would have access to the information.

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

The accuracy of the information in CLM is verified by Master File. Master File receives quarterly updates from the Social Security Administration (SSA) to assist in verifying individual SSNs.

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 36.003	General Personnel and Payroll Records
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File
Treasury .009	Treasury Financial Management Systems

*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? 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?
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?
The information on Master File 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?
Due process is provided at the point of collection of the information, this information is obtained through the processing of federal tax returns. 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. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process.

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 and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Read and Write

Contractor Employees? Yes

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

21.a. How is access to SBU/PII determined and by whom? Access to CLM is granted by Enterprise Operation's Rational Tools Section (RTS) via submission of Online (OL)5081. Approval of the OL5081 provides the user with an account (but not access to any of the CLM repositories). For access to a specific CLM repository, the user then must submit an email request to the three tool process owner's CLM user admin support mailboxes; Enterprise System Testing (EST), Requirements Engineering Program Office (REPO) and Applications Development (AD), requesting access to a specific CLM project area(s) and the role to be provided in each of the three tools that make up CLM (RQM, RTC, DNG). Users with access to restricted CLM repositories must be listed on the projects Live Data Waiver (LDW). The names listed on LDW are referenced against users listed in the restricted CLM repository, and also against OL5081 user information. The project manages the LDW and CLM user access. The review is constant and exceeds the quarterly requirement.

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.

Records are maintained in accordance with General Records Schedule (GRS)3.1, item 011 published in IRS Document 12829.

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. Access is granted and tracked via Online5081 system. The system is used to grant access, password management.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24.b. If no, please explain why. This is a Commercial Off the Shelf (COTs) project.

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?

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. 07/16/2018

25.b. 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:

26.a. IRS Employees:	Not Applicable
26.b. Contractors:	Not Applicable
26.c. Members of the Public:	Under 100,000
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