Date of Approval: August 20, 2018 PIA ID Number: **3577**

## A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. GLDS Task, Request, and Case Management System, TRACMS, TRACMS

2. Is this a new system? No

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

If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

TRACMS, PIAMS # 2656

Enter the approval **date** of the most recent PCLIA. 09/06/2017

If **yes** Indicate which of the following changes occurred to require this update (check all that apply).

No Addition of Personally Identifiable Information (PII)(PII is any information that is linked or linkable).
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
No Expiring PCLIA

Were there other system changes not listed above? No

3. What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym. Privacy, Governmental Liaison & Disclosure/PGLD

3.a. Check the current Enterprise Life Cycle (ELC) Milestones (select all that apply).

No Vision & Strategy/Milestone 0
Yes Project Initiation/Milestone 1
Yes Domain Architecture/Milestone 2
Yes Preliminary Design/Milestone 3
Yes 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.

The Internal Revenue Service (IRS) Office of Governmental Liaison, Disclosure and Safeguards (GLDS) has responsibility for the management of requests for documents pursuant to the Freedom of Information Act (FOIA) and the Privacy Act (PA) and disclosure of tax records under the provisions of Internal Revenue Code (IRC) Section 6103, as well as the responsibility for the activities of the Governmental Liaison and Safeguards programs. GLDS processes approximately 60,000 records requests annually. The GLDS functions are located in geographically dispersed offices throughout the USA. The goal is for the IRS to replace the current client-based application with a web-based application that allows them to electronically receive and process 6103, FOIA, and PA requests; manage inventory; evenly distribute workload nationwide; and track Disclosure, Governmental Liaison, Privacy Policy & Knowledge Management (PP&KM), and Safeguards program work activities. The IRS desires a web-based application that will allow them to electronically receive and process 6103, FOIA, and PA requests; manage inventory; track Disclosure, Governmental Liaison, PP&KM, and Safeguards program work activities: maintain the system and document repository to store and retain program records in a cloud-based environment; contain an online request portal for users and evenly distribute workload nationwide. We have identified requirements for a web-based system to allow the IRS to fulfill requests with greater efficiency, greater consistency and quality of service to our customers and to be in compliance with known and foreseen changes in law. For example, the Open Government Act 2007 requiring changes to the new version of the application to comply with changes in reporting requirements, the FOIA Improvement Act 2016 that mandates the operation of a consolidated online request portal that allows a member of the public to submit a request for records and the Federal Cloud Computing Strategy February 8, 2011 that requires each agency to re-evaluate its technology sourcing strategy to include consideration and application of cloud computing solutions as part of the budget process. The current system is aging and was built on technology that is currently outdated and no longer able to be updated without a platform change. This system currently houses Disclosure casework (for FOIA and other case types), Governmental Liaison daily work, PP&KM daily work, and much of Data Services daily work. The purpose of this project is to define and acquire a web-based, commercial off the shelf (COTS) system that, with some modification, can replace the system functionality of the current system and include all requirements necessary for the addition of Safeguards daily work so that all GLDS functions will use a common electronic solution.

**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 |
| Yes | 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.

There is no known mitigation strategy planned to eliminate the use of SSNs for the system. The SSN is required for the use of this system. The SSN number is needed to research and locate records in response to the request. That said, the display of SSN/EIN information on the user screens will be masked as much as the required use of that data and the technology will allow.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

The display of SSN/EIN information on the user screens will be masked as much as the required use of that data and the technology will allow.

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 |
|---|---|
| Yes | Name |
| Yes | Mailing address |
| Yes | Phone Numbers |
| Yes | E-mail Address |
| Yes | Date of Birth |
| No | Place of Birth |
| Yes | Standard Employee Identifier (SEID) |
| No | Mother's Maiden Name |
| Yes | Protection Personal Identification Numbers (IP PIN) |
| No | Internet Protocol Address (IP Address) |
| Yes | Criminal History |
| Yes | Medical Information |
| Yes | Certificate or License Numbers |
| No | Vehicle Identifiers |
| No | Passport Number |
| No | Alien Number |
| Yes | Financial Account Numbers |
| Yes | Photographic Identifiers |
| No | Biometric Identifiers |
| Yes | 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 |
|---|---|---|
| Yes | Agency Sensitive Information | Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission |
| Yes | 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. |
| Yes | 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 |
| Yes | Physical Security Information | Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities |
| Yes | 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 |
| Yes | SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397 |
| Yes | 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.

The PII needed in this system allows GLDS employees to manage and respond to requests for access to IRS records. Requests can be made under the FOIA, Privacy Act (PA), or IRC 6103. The application requires the SSN to be able to accurately respond to the request. The SSN number is needed to research and locate records in response to the request made under the American Freedom of Information Act.

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

The source of the PII input into the system is the letter provided by the requester seeking access to records. The requester is also required to provide proof of identity for verification. Name, address, and other identifying information is provided to assist in locating the requested information and responding to the request. A number of fields have input and user validation measures to reduce errors. The case number is auto generated during indexing. In addition, the dates, SSN, Employer Identification Number (EIN), years, and other similar fields for which users enter information have specifications for data formats and types. When entered incorrectly the user may be presented with an error message. In addition, employees working a case can verify with the Integrated Data Retrieval System (IDRS) , whether it does or does not have a record relating to that case. The case worker has to be an authorized user and have an account for IDRS. IDRS does not interconnect with TRACMS.

## 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** |
|---|---|
| Treasury/IRS 48.001 | Disclosure Records |
| Treasury/IRS 34.037 | Audit Trail and Security Records System |
| Treasury/IRS 24.030 | Customer Account Data Engine Individual Master File |
| Treasury/IRS 26.046 | Customer Account Data Engine Business Master File |
| Treasury/IRS 36.003 | General Personnel and Payroll Records |
| Treasury/IRS 34.013 | Identification Media Files System for Employees and Others Issued IRS Identification |

*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? Yes

11.a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

| System Name | Current PCLIA | Approval Date | SA&A? | Authorization Date |
|---|---|---|---|---|
| Individual Master File (IMF) | Yes | 03/06/2017 | Yes | 11/06/2017 |
| IDRS | Yes | 08/29/2017 | Yes | 02/06/2018 |
| Business Master File (BMF) | Yes | 03/08/2018 | Yes | 03/13/2018 |
| Transcript Delivery System (TDS) | Yes | 04/20/2018 | Yes | 04/23/2018 |

11.b. 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 |
|---|---|---|
| DOT = Department of Transportation | Email or Secure Data Transfer (SDT) | Yes |
| FFM=Federally Facilitated Marketplace | Email or Secure Data Transfer (SDT) | Yes |
| FED=Federal | Email or Secure Data Transfer (SDT) | Yes |

11.c. Does the system receive SBU/PII from State or local agencies? Yes

If **yes**, for each state and local 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 |
|---|---|---|
| HS=Human Services | Email or Secure Data Transfer (SDT) | Yes |
| DOC=Department of Corrections | Email or Secure Data Transfer (SDT) | Yes |
| AG=Attorney General | Email or Secure Data Transfer (SDT) | Yes |
| CS=Child Support | Email or Secure Data Transfer (SDT) | Yes |
| SBM=State Based Marketplace | Email or Secure Data Transfer (SDT) | Yes |
| HS-ACA=Human Services Affordable Care Act | Email or Secure Data Transfer (SDT) | Yes |
| CDC= Consolidated Data Center | Email or Secure Data Transfer (SDT) | Yes |
| DOR=Department of Revenue | Email or Secure Data Transfer (SDT) | Yes |
| SWA=State Workforce Agency | Email or Secure Data Transfer (SDT) | Yes |
| SWA=TOP=State Workforce Agency Treasury Offset | Email or Secure Data Transfer (SDT) | Yes |

11.d. Does the system receive SBU/PII from other sources? No

11.e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms.

| Form Number | Form Name |
|---|---|
| 706 | United States Estate Tax Return |
| 11-C | Occupational Tax and Registration Return for Wagering |
| 709 | United States Gift (and Generation-Skipping Transfer) Tax Return |
| 720 | Quarterly Federal Excise Tax Return |
| 926 | Return by a U.S. Transferor of Property to a Foreign Corporation |
| 940 | Employer's Annual Federal Unemployment (FUTA) Tax Return |
| 941 | Employer's Quarterly Federal Tax Return |
| 943 | Employer's Annual Federal Tax Return for Agricultural Employees |
| 944 | Employer's Annual Federal Tax Return |
| 990 | Return of Organization Exempt from Income Tax |
| 1040 | US Individual Income Tax Return |
| 1041 | U.S. Income Tax Return for Estates and Trusts |
| 1042 | Annual Withholding Tax Return for U.S. Source Income of Foreign Persons |
| 1065 | U.S. Return of Partnership Income |
| 1120 | U.S. Corporation Income Tax Return |

11.f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? Yes

If **yes**, identify the forms.

| Form Number | Form Name |
|---|---|
| 6166 | United States Residence Certification |

## F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? No

12.b. Does this system disseminate SBU/PII to other Federal agencies? Yes

If **yes** identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

| Organization Name | Transmission method | ISA/MOU |
|---|---|---|
| FFM = Federally Facilitated Marketplace | Email or Secure Data Transfer (SDT) | Yes |
| DOT = Department of Transportation | Email or Secure Data Transfer (SDT) | Yes |

Identify the authority. 26 CFR 301.6103 - IRC Section 6103 • 6103(d) Disclosure to State tax officials and State and local law enforcement agencies • 6103(h) Disclosure to certain Federal officers and employees for purposes of tax administration, etc. • 6103(i) Disclosure to Federal officers or employees for administration of Federal laws not relating to tax administration The 6103(d) exchanges between State and local agencies are defined by a State or local agency specific Basic Agreement and Implementing Agreement.

Identify the routine use in the applicable SORN (or Privacy Act exception). IRM 11.3.32.5 Basic Agreements - The basic agreement provides for the mutual exchange of tax data between a specific state tax agency and the IRS. The provisions of the basic agreement

encompass required procedures and safeguards. • IRM 11.3.32-3 Implementing Agreements - The purpose of this agreement is to provided implementing procedures for the Agreement on Coordination of Tax Administration between the Internal Revenue Service and xxxxxxxx (hereafter referred to as the "Agency").

For what purpose? Agency data exchanges are for the purpose of tax administration or for 6103(i) to assist with investigations of Federal crimes.

12.c. Does this system disseminate SBU/PII to State and local agencies? Yes

If **yes**, identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

| Organization Name | Transmission method | ISA/MOU |
|---|---|---|
| **DOC = Department of Corrections** | **DOC = Department of Corrections** | **Yes** |
| **DOR = Department of Revenue** | **DOR = Department of Revenue** | **Yes** |
| **CDC = Consolidated Data Center** | **E-mail or Secure Data Transfer** | **Yes** |
| **AG = Attorney General** | **E-mail or Secure Data Transfer** | **Yes** |
| **SWA = State Workforce Agency** | **E-mail or Secure Data Transfer** | **Yes** |
| **CS = Child Support** | **E-mail or Secure Data Transfer** | **Yes** |
| **SBM = State Based Marketplace** | **E-mail or Secure Data Transfer** | **Yes** |
| **HS¬-ACA = Human Services Affordable Care Act** | **E-mail or Secure Data Transfer** | **Yes** |
| **SWA-TOP = State Workforce Agency Treasury Offset Program** | **E-mail or Secure Data Transfer** | **Yes** |
| **HS = Human Services** | **E-mail or Secure Data Transfer** | **Yes** |

Identify the authority. 26 CFR 301.6103 - IRC Section 6103 • 6103(d) Disclosure to State tax officials and State and local law enforcement agencies • 6103(h) Disclosure to certain Federal officers and employees for purposes of tax administration, etc. • 6103(i) Disclosure to Federal officers or employees for administration of Federal laws not relating to tax administration The 6103(d) exchanges between State and local agencies are defined by a State or local agency specific Basic Agreement and Implementing Agreement.

Identify the routine use in the applicable SORN (or Privacy Act exception.) IRM 11.3.32.5 Basic Agreements - The basic agreement provides for the mutual exchange of tax data between a specific state tax agency and the IRS. The provisions of the basic agreement encompass required procedures and safeguards.

For what purpose? Agency data exchanges are for the purpose of tax administration or for 6103(i) to assist with investigations of Federal crimes.

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? Yes

If **yes**, identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

| Organization Name | Transmission method | ISA/MOU |
|---|---|---|
| Awarded System Developer | Direct use of IRS Systems as Necessary | No |

Identify the authority PRIVACY ACT NOTIFICATION (APR 1984) The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties. In accordance with Homeland Security Presidential Directive 12 (HSPD-12), the Department of the Treasury Security Manual, Chapter II,

Section 2, Investigative Requirements for Contractor Personnel describes "investigative requirements for contract employees, subcontractors, experts, and consultants who require staff-like access, wherever the location, to (1) Treasury/bureau-owned or controlled facilities; or (2) work on contracts that involve the design, operation, repair or maintenance of information systems; and/or (3) require access to sensitive but unclassified (SBU) information." Internal Revenue Manual (IRM) 10.8.1, Information Technology (IT) Security Policy and Guidance, establishes comprehensive, uniform security policies for the IRS. This manual applies to individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate IT systems containing IRS data. Pursuant to IRSAP clause IR1052.239-9007, the contractor is required to furnish the Contracting Officer's Representative (COR) a list of names (as well as any other requested, supporting information) of new or substitute contractor employees and the IRS locations for which access is requested. A security screening, if determined appropriate by the IRS and in accordance with IRM 10.23.2, Personnel Security, Contractor Investigations, and TD P 15-71, Chapter II, Section 2, will be conducted by IRS for each contractor employee requiring access to IRS' IT systems, or as otherwise deemed appropriate by the COR. Unless otherwise stated in Treasury regulation, the information shall be submitted within five (5) days of contract award and within 24 hours of the date that the identity of a prospective personnel substitution has been confirmed. In addition to the requirements set forth above, the contractor shall also comply with the following IRS clauses: 1. IR1052.204-9003, IRS Security Awareness Training Requirements 2. IR1052.204-9005, Submission of Security Forms and Related Materials 3. IR1052.204-9006, Notification of Change in Contractor Employee Employment Status, Assignment, or Standing 4. IR1052.239-9007, Access, Use or Operation of IRS Information Technology (IT) Systems by Contractors

For what purpose? Contractor support is required for planning, managing, and executing the design, build, test, and deployment phases of the proposed system. As such, the contractor will be expected to finalize business requirements, develop necessary design specifications, modify the application to meet requirements, develop and execute software testing and data validation to ensure quality deliverables, develop and execute a plan for data conversion, provide system documentation for operation and maintenance support, provide assistance as needed with any FISMA / IT security activities and documentation.
Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?>
Yes

12.e. Does this system disseminate SBU/PII to other Sources? Yes

If **yes**, identify the other source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

| Organization Name | Transmission method | ISA/MOU |
|---|---|---|
| FOIA requestor | Web Portal | No |

Identify the authority 26 CFR 301.6103 - IRC Section 6103 • 6103(d) Disclosure to State tax officials and State and local law enforcement agencies • 6103(h) Disclosure to certain Federal officers and employees for purposes of tax administration, etc. • 6103(i) Disclosure to Federal officers or employees for administration of Federal laws not relating to tax administration The 6103(d) exchanges between State and local agencies are defined by a State or local agency specific Basic Agreement and Implementing Agreement.

Identify the routine use in the applicable SORN (or Privacy Act exception) IRM 11.3.32.5 Basic Agreements - The basic agreement provides for the mutual exchange of tax data between a specific state tax agency and the IRS. The provisions of the basic agreement encompass required procedures and safeguards.

For what purpose? The proposed TRACIMS system will allow the Office of Disclosure to utilize a web portal. The FOIA requestor will have the ability to select their desired delivery method, by postal mail, email, or web portal. Once Disclosure has designated documents for release, the web portal will allow the FOIA requestors to securely retrieve responsive documents designated for release to the designated requestor.

## 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? Yes

15.a. If **yes**, Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified? Yes

If **yes**, Date Certified. 02/21/2014

15.b. Please identify the ownership of CSP data. IRS

15.c. Does the CSP allow auditing? Yes

Who audits the CSP data? IRS

15.d. Please select background check level required for CSP. High

15.e. Is there a breach/incident plan on file? Yes

15.f. Privacy laws (including access and ownership) can differ in other countries. If any data is considered SBU, will this cloud be Continental US (CONUS) only for:

| | |
|---|---|
| Storage | Yes |
| Transmission | Yes |
| Maintenance (including backups) | Yes |
| Troubleshooting | Yes |

16. Does this system/application interact with the public? Yes

16.a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

16.a.1. If **yes**, when was the **e-RA** conducted? 07/11/2017

If **yes**, what was the approved level of authentication?

Level 4: Very High confidence in the asserted identity's validity.

## 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?
In order to make a request under the Freedom of Information Act, the source of the PII input into the system is a letter provided by the individual requester seeking access to records. Name, address, and other identifying information is provided to assist in locating the requested information and responding to the request.

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 collected under the Freedom of Information Act, is required to perform the search of requested records. Individuals do not have the opportunity to decline from providing the required information. In order to initiate a FOIA request the guidelines laid out in the "How to file a FOIA" section of the Internal Revenue website explicitly states the following: IRS has prepared a document at Appendix A- "How to Make a Freedom of Information Act Request" that describes the request process in greater detail. A requester who follows the IRS's specific procedures may receive a faster response. There are four basic elements to a FOIA request letter: First, the letter should state that the request is being made under the Freedom of Information Act. Second, the request should identify the records that are being sought as specifically as possible. Third, the name and address of the requester must be included along with a copy of the requester's driver's license or a sworn or notarized statement swearing to or affirming their identity if the request involves the tax records of an individual or a business. In this case, the authority of the requester to receive such records must be established. NOTE: FOIA requests seeking a Centralized Authorization File (CAF) Client Listing must attach a valid photo identification, including a signature. IRS will accept no other method of establishing identity for these requests. Fourth, the requester should make a firm commitment to pay any fees which may apply (the complete regulatory requirements for FOIA requests filed with the IRS are available at 67 Federal Register 69673, Treasury Regulation 601.702). https://www.irs.gov/uac/freedom-of-information-act-foia-guidelines In addition regarding the Safeguard segment of the application the information is not collected directly from individuals. The information collected by state/local or federal agencies is obtained via TDS and subsequently provided to Safeguards to justify protection of Federal Tax Information (FTI). Notice, consent and due process are provided via TDS and its related tax forms and instructions, and pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress? The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant 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 Contractor 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-Only |

Contractor Employees? Yes

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

21.a. How is access to SBU/PII determined and by whom? When a new user needs access to IRS systems or applications, the user's manager or designated official, accesses the Online 5081 (OL5081) application to request access for the new user. The completed OL5081 is submitted to the application administration approval group, and then the user is added by their Standard Employee Identification (SEID). Access to the data within the application is restricted. Users are restricted to only those pieces of the application to which they need access by permissions and workgroup assignments. Users such as case workers only have access to input data for their work group assignment, run pre-programmed reports and ad hoc queries, and cannot delete data or records or manipulate or physically access the data. Access to the data tables is restricted to the application, system, and database administrators.

## 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.

The system data retention requirements follow Records Control Schedule 1. Access and disclosure request files, Case files created in response to FOIA requests a.) General Records Schedule (GRS) 4.2/020 ; Case files created in response to requests for information under the Freedom of Information Act (FOIA), Mandatory Declassification Review (MDR) process, Privacy Act (PA), Classification Challenge, and similar access programs (Job No. DAA-GRS-2013-0007-0002) b.) Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for

business use. 2. Requests for Return and Return Information Files; Files consist of requests for copies or inspection of confidential tax returns or return information; either hard copy or tape extracts, and related records or actions taken (Job No. N1-58-05-2, Item 52) a.) RCS 8/52; Implementation Agreements and Memoranda of Understanding (MOU). These include Basic Agreements BAs, Implementing Agreements IAs, Memoranda of Agreements MOAs, Interagency Exchange Agreements IEAs, Letters of Agreement LOA and any form of inter-agency agreement signed by participating agencies. b.) PGLD facilitates the exchange of data and fosters partnerships with federal, state, and local governmental agencies to improve tax administration, in accordance with Policy Statement 11-98, FedState Relations. See IRM 1.2.19.1.13, Policy Statement 11-98 (Formerly P-6-14). i.) Record Copy - Paper ib.) Destroy paper 3 years after receipt of new or amended agreement ii.) Electronic Copies. Records in the above series that may have been created using word processing, e-mail, or some other electronic application. Copies that have no further administrative value after the recordkeeping copy is made. This includes copies maintained by individuals in personal files, electronic mail directories, or other directory on hard disk or network drives and copies on shared network drives used only to produce the recordkeeping copy. iib.) Destroy/Delete within 180 days (6 months) after the recordkeeping copy has been made or no longer needed. iii.) Electronic Copies. Records in the above series that may have been created using word processing, e-mail, or some other electronic application. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. iiib.) Destroy/Delete when dissemination, revision, or updating is complete. iv.) All other offices/copies (paper and electronic). ivb.) Destroy after reading, or within 30 days, whichever is sooner 3.) Disclosure of Information to Federal, State, and Local Agencies (DIFSLA). a.) Matching and Extract Program RCS 19/58 Disclosure of Information to Federal, State and Local Agencies (DIFSLA) matching and extract program was developed pursuant to IRC 6103(1)(7) and IRC 6103(1)(7)(8) and includes Federal and State agencies authorized to participate in the program. IRS provides agencies with income information for use in determining benefit program eligibility. DIFSLA allows participating Federal, State, and Local Agencies to request data for use in public assistance programs. Agencies submit Social Security Number (SSN) which are validated against the National Account Profile (NAP) file and matched against the Information Returns Master File Processing System (IRMF) documents. Matches showing unearned-income are extracted. (Job No. N1-58-09-41). i.) Inputs: Disclosure of Information to Federal, State, and Local Agencies (DIFSLA) ib.) Delete/Destroy any cached input files, data, and reports immediately following validation of receipts by the system and/or receipt by the agency. ii.) System Data: Contents of the Disclosure of Information to Federal, State, and Local Agencies (DIFSLA) System include, but not limited to the following extracts; GLDSEP, 1099-MISC, Business Master File (BMF) and Business Return Transaction File (BRTF), Corporate Affiliations, CP2000, Exam/Appeals, Federal Employer Identification Number (FEIN), Individual Master File (IMF)/Individual Returns Transaction Files (IRTF), Individual Taxpayer Identification Number (ITIN), Information Returns Master File (IRMF), LEVY, Military Combat Zone, Non-Itemizer, Preparer Tax Identification Number (PTIN), Taxpayer Address Record (TAR), and a tickler file, or tickler tape, input file that is merged with IRS data to produce a specific data extract. iib.) Cut off at end of the processing year. Delete/Destroy 5 years after cutoff. iii.) Outputs: Outputs from the Disclosure of Information to Federal, State, and Local Agencies (DIFSLA) Systems are on magnetic media in which the tax return information about identified individuals is provided on cartridge(s) by the IRS. Outputs include Extracts Data extracted from the Wage and Information Returns (IRP) File - Treasury/IRS 22.061, referred to as the Information Returns Master File (IRMF) for the current tax year. This file contains information returns filed by payers of income such as dividends, interest and retirement income as reported on Forms 1099-DIV, 1099-INT and 1099-R, respectively. The information is extracted on a monthly basis using identifying information on magnetic media submitted by the requester. DIFSLA also electronically transfers information to Information Returns Master File Processing System (IRMF). Note: The data warehouses and repositories of target systems house the official records for all outputs from the DIFSLA. These are appropriately scheduled under approvals cited in the various Records Control Schedules of the Internal

Revenue Service. iiib.) Delete/Destroy any cached input files, data, and reports immediately following validation of outcomes to target systems and agencies. iv.) System Documentation: System Documentation for the Disclosure of Information to Federal, State, and Local Agencies (DIFSLA) System consists of codebooks, records layout, user guide, and other related materials. ivb.) Delete/Destroy when superseded or 5 years after the system is terminated, whichever is sooner. Regarding Safeguards segment, the status of Safeguards reports/case files already scheduled under Job No. N1-58-00-1, and published in IRS Document 12990 under Records Control Schedule (RCS) 8, item 101. For Safeguards Procedures Reports (SPR) - destroy after 2 subsequent SPRs are received. Safeguards Activity Reports (SAR) Destroy when 5 years old. Both the SPR and SAR have been replaced by the Safeguards Security Reports (SSR) as of January 2014. SSRs will be destroyed when 5 years old. Safeguards Review Reports - SRR (Record Copy destroy after 2 subsequent reviews are completed. Reference/Management Records are destroyed when 3 years old. Any new records identified will be scheduled in coordination with the IRS Records Officer and the RIM Office. (RIM) Program Office, and submitted to the National Archives and Records Administration (NARA) for disposition approval.

## I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? In-process

23.b. If **in process**, when is the anticipated date of the SA&A or ASCA completion? 10/01/2018

23.1 Describe in detail the system's audit trail. Due to the TRACMS project being assigned to the Managed Services Path, the auditing functions will be conducted by the vendor in compliance with IRM 2.16.1.4.3.3 (07-10-2017), Managed Services Path.

## J. PRIVACY TESTING

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

24.b. If **no**, please explain why. All the customer configurable security controls are implemented as intended and documented in the TRACMS System Security Plan (SSP).

## K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

## L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

| | |
|---|---|
| 26.a. IRS Employees: | Under 50,000 |
| 26.b. Contractors: | Under 5,000 |
| 26.c. Members of the Public: | 100,000 to 1,000,000 |
| 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? Yes

27.a. If **yes**, explain the First Amendment information being collected and how it is used. While systems do not collect this information exclusively, the tax returns stored in the database will include information related to First Amendment rights, such as charitable contributions or income/deductions for such activities.

27.b. If **yes**, please check all of the following exceptions (any one of which allows the maintenance of such information) that apply:

There is a statute that expressly authorizes its collection. (Identified in Q6) Yes

27.c. If **yes**, will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges under Federal programs? 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? Yes

31.a. does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact *Disclosure* to determine if an accounting is required. Yes

**End of Report**