

Date of Approval: **February 04, 2020**

PIA ID Number: **4703**

## **SYSTEM DESCRIPTION**

*Enter the full name and acronym for the system, project, application and/or database.*

GLDS Reimbursables Data Exchange, GLDS RA

*Is this a new system?*

No

*Is there a PCLIA for this system?*

Yes

*What is the full name, acronym and milestone of the most recent PCLIA?*

GLDS Reimbursables Data Exchange, GLDS RA, Operations and Maintenance. # 2234

*What is the approval date of the most recent PCLIA?*

4/3/2017

*Changes that occurred to require this update:*

Expiring PCLIA

*Were there other system changes not listed above?*

No

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

Privacy, Governmental Liaison and Disclosure (PGLD)

*Current ELC (Enterprise Life Cycle) Milestones:*

Operations & Maintenance (i.e. system is currently operational)

*Is this a Federal Information Security Management Act (FISMA) reportable system?*

No

## GENERAL BUSINESS PURPOSE

*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 Governmental Liaison, Disclosure and Safeguards (GLDS) Reimbursables Data Exchange system has a government mandate to share data with other federal, state and local agencies pursuant to Internal Revenue Code (IRC) 6103 which allows participating agencies to request unearned income data for use in administering federal benefits programs pursuant IRC 6103(1)(7). The system also allows specific agencies to request the latest taxpayer address information upon availability via the Individual Master File (IMF) pursuant IRC 6103(1)(6), (m)(2), (3), and (7). Agencies submit social security numbers (SSNs), along with name controls, via tickler (Flat) files. These files are logged by the Electronic File Transfer Utility (EFTU) and record counts are monitored to ensure records sent by the agency match what is received by the IRS. Tickler files are validated and matched via batch processing (no direct access) to the Information Return Master File (IRMF) for Disclosure of Information to Federal, State & Local Agencies (DIFSLA) and to the IMF for Taxpayer Address Requests (TAR). Data is extracted and transferred to a secure folder where the participating agency can then access the specific information requested. The Office of Governmental Liaison, Disclosure and Safeguards (GLDS) executes a computer matching agreement (CMA) with each agency participating in the data exchanges to allow the parties to engage in the data exchange. Participating agencies include six federal agencies and 52 state agencies.

## PII DETAILS

*Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?*

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

*What types of tax identification numbers (TIN) apply to this system?*

Social Security Number (SSN)

*List the approved Treasury uses of the SSN:*

Delivery of governmental benefits, privileges, and services

*Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)*

The Governmental Liaison, Disclosure and Safeguards (GLDS) Reimbursables Data Exchange system has a government mandate to share data with other federal, state and local agencies pursuant to 6103(l)(7), 6103(l)(6), 6103(m)(2), 6103(m)(3) and 6103(m)(7).

*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 Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use Social Security Numbers (SSNs), which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The GLDS Reimbursables Data Exchange system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

*Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?*

Yes

*Specify the PII Elements:*

Name

Mailing address

Tax Account Information

*Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?*

Yes

*Specify the types of SBU from the SBU Types List*

Proprietary data    Business information that does not belong to the IRS

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

*Are there other types of SBU/PII used in the system?*

Yes

*Describe the other types of SBU/PII that are applicable to this system.*

Federal Tax Information

*Cite the authority for collecting SBU/PII (including SSN if relevant)*

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

*Has the authority been verified with the system owner?*

Yes

## **BUSINESS NEEDS AND ACCURACY**

*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.*

By law, data must be released to federal, state and local agencies that have a justified need. No data is released unless it is permitted by statute. Disclosure of Information to Federal, State and Local Agencies (DIFSLA) - IRC 6103(l)(7) authorizes IRS to disclose return information with respect to unearned income to federal, state and local agencies administering certain benefit programs under the Social Security Act. Medicare Prescription Drug Subsidy Program - IRC 6103(l)(7) authorizes IRS to disclose return information with respect to unearned income to federal, state and local agencies administering certain benefit programs under the Social Security Act. Medicare Part B Premium Reduction - IRC 6103(l)(20) authorizes the IRS to disclose specified return information to the Social Security Administration with respect to taxpayers whose Part B insurance premium may, according to IRS records, be subject to adjustments. Taxpayer Address Requests (TAR) - IRC 6103(m)(2), (3), (5), and (7) - IRC 6103(m)(2) authorizes IRS to disclose the mailing address of a taxpayer for use by officers, employees, or agents of a federal agency for purposes of locating such taxpayer to collect or compromise a federal claim against the taxpayer in accordance with sections 3711, 3717, and 3718 of title 31. IRC 6103(m)(3) authorizes IRS to disclose the mailing address of taxpayers to officers and employees of the National Institute

for Occupational Safety and Health solely for the purpose of locating individuals who are, or may have been, exposed to occupational hazards in order to determine the status of their health or to inform them of the possible need for medical care and treatment. IRC 6103(m)(7) authorizes IRS to disclose the mailing address of any taxpayer who is entitled to receive a social security account statement pursuant to section 1143(c) of the Social Security Act, for use only by officers, employees or agents of the Social Security Administration for purposes of mailing such statement to such taxpayer. IRC 6103(l)(6) authorizes IRS to disclose address information solely for purposes of, and to the extent necessary in, establishing and collecting child support obligations from, and locating, individuals owing such obligations. The system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

*How is the SBU/PII verified for accuracy, timeliness and completion?*

The correctness of the return information provided to the Agency is generally contingent upon the correctness of the information provided by the payer of the income. Pursuant U.S.C. section 552a(p) and noted in the computer matching agreement document: Notice and Opportunity to Contest 1. Where adverse information is uncovered, the agency will notify the applicant or recipient, and provide an opportunity to explain the circumstances prior to making a final eligibility determination or adjustment to current benefits. 2. The individual subject to adverse action shall be provided a minimum of 30 days to contest the action, unless (1) the Federal Benefit program involved in the match has its own time period for contesting an adverse action or (2) the situation falls under the exception for situations when an agency determines there is likely to be a significant effect on public health or safety. 5 U.S.C. 552a(p)(3).

## **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.

*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

*Identify the Privacy Act SORN(s) that cover these records.*

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 34.037 Audit Trail and Security Records

## **RESPONSIBLE PARTIES**

*Identify the individuals for the following system roles:*

## Official Use Only

## **INCOMING PII INTERFACES**

*Does the system receive SBU/PII from other systems or agencies?*

Yes

*Does the system receive SBU/PII from IRS files and databases?*

Yes

*Enter the files and databases:*

System Name: Individual Master File ( IMF )

Current PCLIA: Yes

Approval Date: 3/26/2019

SA&A: Yes

ATO/IATO Date: 9/22/2019

*Does the system receive SBU/PII from other federal agency or agencies?*

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).*

Name: National Institute of Occupational Safety and Health

Transmission Method: EFTU via Secure Data Transfer

ISA/MOU: Yes

Name: Social Security Administration  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Name: Veterans Benefits Administration  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Name: Veterans Health Administration  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Name: Department of Justice  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Name: Office of Child Support Enforcement  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

*Does the system receive SBU/PII from State or local agency (-ies)?*

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: Alabama Department of Human Resources  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Alabama Medicaid Agency  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Alaska Department of Health and Social Services, Division of Public Assistance  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Arizona Department of Economic Security  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Arkansas Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: California Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Connecticut Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Delaware Department of Health and Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: District of Columbia Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Florida Department of Children and Families  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Georgia Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Hawaii Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Idaho Department of Health and Welfare  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Illinois Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Indiana Family and Social Services Administration  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes



Organization Name: Iowa Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Kansas Department for Children and Families  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Kentucky Cabinet for Health and Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Louisiana Department of Children and Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Louisiana Department of Health  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Maine Department of Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Maryland Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Massachusetts Department of Transitional Assistance  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Michigan Department of Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Minnesota Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Mississippi Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Mississippi Division of Medicaid  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Missouri Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Montana Department of Public Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Nebraska Department of Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: New Hampshire Department of Health and Human Services, Division of Family Assistance  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: New Jersey Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: New Mexico Human Services Department  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: New York Office of Temporary and Disability Assistance  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: North Carolina Department of Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: North Dakota Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Ohio Department of Jobs and Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Ohio Department of Medicaid  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Oklahoma Department of Human Services, Adult and Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Oregon Department of Human Services, Health Authority  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Pennsylvania Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Rhode Island Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: South Carolina Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: South Dakota Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Tennessee Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Texas Health and Human Services Commission  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Utah Department of Workforce Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Vermont Department for Children and Families, Economic Services  
Division  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Virginia Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Washington Department of Social and Health Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Wisconsin Department of Children and Families  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Wyoming Department of Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

*Does the system receive SBU/PII from other sources?*

No

*Does the system receive SBU/PII from Taxpayer forms?*

No

*Does the system receive SBU/PII from Employee forms (e.g. the I-9)?*

No

## **DISSEMINATION OF PII**

*Does this system disseminate SBU/PII?*

Yes

*Does this system disseminate SBU/PII to other IRS Systems?*

No

*Does this system disseminate SBU/PII to other Federal agencies?*

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: Veterans Benefits Administration  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes*

*Organization Name: Veterans Health Administration  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes*

*Organization Name: Department of Justice  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes*

*Organization Name: Office of Child Support Enforcement  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes*

*Organization Name: Social Security Administration  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes*

*Organization Name: National Institute of Occupational Safety and Health  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes*

*Identify the authority*

Disclosure of Information to Federal, State and Local Agencies (DIFSLA): IRC 6103(l)(7) authorizes the use of certain return information by agencies administering certain programs under the Social Security Act. Medicare Prescription Drug Subsidy Program - IRC 6103(l)(7) authorizes IRS to disclose return information with respect to unearned income to federal, state and local agencies administering certain benefit programs under the Social Security Act. Medicare Part B Premium Reduction - Section 6103(l)(20) authorizes the IRS to disclose specified return information to SSA with respect to taxpayers whose Part B insurance premium may, according to IRS records, be subject to adjustments. Taxpayer Address Requests (TAR) - IRC 6103(m) authorizes the disclosure of the taxpayer mailing addresses to locate individuals to collect or compromise federal claims, for defaulted student loans and other specified uses.

*Identify the Routine Use in the applicable SORN (or Privacy Act exception)*

SORN 24.030 Treas/IRS Customer Account Data Engine (CADE) Individual Master File (IMF) - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the

purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted. To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. SORN 24.046 Treas/IRS Customer Account Data Engine (CADE) Business Master File (BMF) - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted. To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. SORN 34.037 Treas/IRS IRS Audit Trail and Security Records - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted. (1) Disclose information to the Department of Justice (DOJ) when seeking legal advice or for use in any proceeding, or in preparation for any proceeding, when: (a) The IRS or any component thereof; (b) any IRS employee in his or her official capacity; (c) any IRS employee in his or her individual capacity if the IRS or DOJ has agreed to provide representation for the employee; or (d) the United States is a party to, has an interest in, or is likely to be affected by, the proceeding and the IRS determines that the records are relevant and necessary to the proceeding or advice sought. (2) Disclose information in a proceeding (including discovery) before a court, administrative tribunal, or other adjudicative body when: (a) The IRS or any component thereof; (b) any IRS employee in his or her official capacity; (c) any IRS employee in his or her personal capacity if the IRS or DOJ has agreed to provide representation for the employee; or (d) the United States is a party to, has an interest in, or is likely to be affected by, the proceeding and the IRS or DOJ determines that the information is relevant and necessary to the proceeding. Information may be disclosed to the adjudicative body to resolve issues of relevancy, necessity, or privilege pertaining to the information. (3) Disclose information to an appropriate Federal, state, local, tribal, or foreign agency, or other public authority, responsible for implementing or enforcing, or for investigating or prosecuting the violation of, a statute, rule, regulation, order, or license, when a record on its face, or in conjunction with other records, indicates a potential violation of law or regulation and the information disclosed is relevant to any regulatory, enforcement, investigative, or

prosecutorial responsibility of the receiving authority. (4) Disclose information to officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation. (5) Disclose information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation. (6) Disclose information to a contractor, including an expert witness or a consultant, hired by the IRS, to the extent necessary for the performance of a contract. (7) To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

*For what purpose?*

SORN 24.030 Treas/IRS Customer Account Data Engine (CADE) Individual Master File (IMF) - To maintain records of tax returns, return transactions, and authorized taxpayer representatives. SORN 24.046 Treas/IRS Customer Account Data Engine (CADE) Business Master File (BMF) - To maintain records of business tax returns, return transactions, and authorized taxpayer representatives. SORN 34.037 Treas/IRS IRS Audit Trail and Security Records - To identify and track any unauthorized accesses to sensitive but unclassified information and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy (e.g., gambling, playing computer games, or engaging in illegal activity), or to detect electronic communications sent using IRS systems in violation of IRS security policy.

*Does this system disseminate SBU/PII to State and local agencies?*

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: Kansas Department for Children and Families  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU Yes

Organization Name: Kentucky Cabinet for Health and Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU Yes

Organization Name: Louisiana Department of Children and Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Louisiana Department of Health  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Maine Department of Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Maryland Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Massachusetts Department of Transitional Assistance  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Michigan Department of Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Minnesota Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Mississippi Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Mississippi Division of Medicaid  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Missouri Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Montana Department of Public Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes



Organization Name: Nebraska Department of Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: New Hampshire Department of Health and Human Services, Division of Family Assistance  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: New Jersey Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: New Mexico Human Services Department  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: New York Office of Temporary and Disability Assistance  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Wyoming Department of Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Alabama Department of Human Resources  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Alabama Medicaid Agency  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Alaska Department of Health and Social Services, Division of Public Assistance  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Arizona Department of Economic Security  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Arkansas Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: California Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Connecticut Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Delaware Department of Health and Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: District of Columbia Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Florida Department of Children and Families  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Georgia Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Hawaii Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Idaho Department of Health and Welfare  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Illinois Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Indiana Family and Social Services Administration  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Iowa Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: North Carolina Department of Health and Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: North Dakota Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Ohio Department of Jobs and Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Ohio Department of Medicaid  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Oklahoma Department of Human Services, Adult and Family Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Oregon Department of Human Services, Health Authority  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Pennsylvania Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Rhode Island Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: South Carolina Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: South Dakota Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Tennessee Department of Human Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Texas Health and Human Services Commission  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Utah Department of Workforce Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Vermont Department for Children and Families, Economic Services Division  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Virginia Department of Social Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Washington Department of Social and Health Services  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

Organization Name: Wisconsin Department of Children and Families  
Transmission Method: EFTU via Secure Data Transfer  
ISA/MOU: Yes

*Identify the authority*

Disclosure of Information to Federal, State and Local Agencies (DIFSLA): IRC 6103(l)(7) provides for the use of certain return information by agencies administering certain programs under the Social Security Act. Medicare Prescription Drug Subsidy Program - IRC 6103(l)(7) authorizes IRS to disclose return information with respect to unearned income to federal, state and local agencies administering certain benefit programs under the Social Security Act. Medicare Part B Premium Reduction - Section 6103(l)(20) of the Internal Revenue Code authorizes the IRS to disclose specified return information to SSA with respect to taxpayers whose Part B insurance premium may, according to IRS records, be subject to adjustments. Taxpayer Address Requests (TAR) - provides taxpayer mailing addresses. IRC 6103 authorizes the disclosure of the taxpayer mailing address to locate individuals to collect or compromise federal claims, for defaulted student loans and other specified uses 6103(m).

*Identify the Routine Use in the applicable SORN (or Privacy Act exception)*

SORN 24.030 Treas/IRS Customer Account Data Engine (CADE) Individual Master File (IMF) - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records,

and no privilege is asserted. To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. SORN 24.046 Treas/IRS Customer Account Data Engine (CADE) Business Master File (BMF) - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted.

To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. SORN 34.037 Treas/IRS IRS Audit Trail and Security Records - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted.

(1) Disclose information to the Department of Justice (DOJ) when seeking legal advice or for use in any proceeding, or in preparation for any proceeding, when: (a) The IRS or any component thereof; (b) any IRS employee in his or her official capacity; (c) any IRS employee in his or her individual capacity if the IRS or DOJ has agreed to provide representation for the employee; or (d) the United States is a party to, has an interest in, or is likely to be affected by, the proceeding and the IRS determines that the records are relevant and necessary to the proceeding or advice sought.

(2) Disclose information in a proceeding (including discovery) before a court, administrative tribunal, or other adjudicative body when: (a) The IRS or any component thereof; (b) any IRS employee in his or her official capacity; (c) any IRS employee in his or her personal capacity if the IRS or DOJ has agreed to provide representation for the employee; or (d) the United States is a party to, has an interest in, or is likely to be affected by, the proceeding and the IRS or DOJ determines that the information is relevant and necessary to the proceeding. Information may be disclosed to the adjudicative body to resolve issues of relevancy, necessity, or privilege pertaining to the information.

(3) Disclose information to an appropriate Federal, state, local, tribal, or foreign agency, or other public authority, responsible for implementing or enforcing, or for investigating or prosecuting the violation of, a statute, rule, regulation, order, or license, when a record on its face, or in conjunction with other records, indicates a potential violation of law or regulation and the information disclosed is relevant to any regulatory, enforcement, investigative, or prosecutorial responsibility of the receiving authority.

(4) Disclose information to officials of

labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation. (5) Disclose information to third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation. (6) Disclose information to a contractor, including an expert witness or a consultant, hired by the IRS, to the extent necessary for the performance of a contract. (7) To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

*For what purpose?*

SORN 24.030 Treas/IRS Customer Account Data Engine (CADE) Individual Master File (IMF) - To maintain records of tax returns, return transactions, and authorized taxpayer representatives. SORN 24.046 Treas/IRS Customer Account Data Engine (CADE) Business Master File (BMF) - To maintain records of business tax returns, return transactions, and authorized taxpayer representatives. SORN 34.037 Treas/IRS IRS Audit Trail and Security Records - To identify and track any unauthorized accesses to sensitive but unclassified information and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy (e.g., gambling, playing computer games, or engaging in illegal activity), or to detect electronic communications sent using IRS systems in violation of IRS security policy.

*Does this system disseminate SBU/PII to IRS or Treasury contractors?*

No

*Does this system disseminate SBU/PII to other Sources?*

No

## **PRIVACY SENSITIVE TECHNOLOGY**

*Does this system use social media channels?*

No

*Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?*

No

*Does the system use cloud computing?*

No

*Does this system/application interact with the public?*

No

## **INDIVIDUAL NOTICE AND CONSENT**

*Was/is notice provided to the individual prior to collection of information?*

Yes

*How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?*

When an individual is applying for benefits, they sign a document regarding acquiring data from other federal and state agencies to determine the correct amount of benefits. Constructive notice is also given by publishing notice of the matching program via the Federal Register.

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

Yes

*Describe the mechanism by which individuals indicate their consent choice(s):*

When an individual is applying for assistance, they sign a document regarding acquiring data from other federal and state agencies to determine the correct amount of benefits. Constructive notice is also given by publishing the matching program via the Federal Register.

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

As noted in computer matching agreements with federal, state and local agencies: Notice and Opportunity to Contest 1. Where adverse information is uncovered, the agency will notify the applicant or recipient, and provide an opportunity to explain the circumstances prior to making a final eligibility determination or adjustment to current benefits. 2. The individual subject to adverse action shall be provided a minimum of 30 days to contest the action, unless (1) the Federal Benefit Program involved in the match has its own time period for contesting an adverse action or (2) the situation falls under the exception for situations when an agency determines there is likely to be a significant effect on public health or safety. 5 U.S.C. 552a(p)(3).

## **INFORMATION PROTECTION**

*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

*The following people have access to the system with the specified rights:*

*IRS Employees*

System Administrators: Read Write

Developers: Read Write

*How is access to SBU/PII determined and by whom?*

Data access is granted on a need-to-know basis. A potential user must submit a request for access via the IRS Online 5081 (OL5081) application. The requested access must be approved or denied by the user's authorized management official. Access is only permitted with the authorized management official's acknowledgement of access approval via OL5081. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the OL5081 application and set (activated) by the system administrator prior to the user being allowed and granted access. User privileges and user roles determine the types of data that each user has permission to access. Management, as well as system administrators, monitors system access and removes permissions when individuals no longer require access. Participating agencies must have a computer matching agreement in place to participate and are subject to reviews by the IRS Safeguards to ensure they comply with Internal Revenue Code (IRC) 6103 (p)(4). They must comply with the Computer Matching and Privacy Protection Act and IRC 6103(p)(4) in order to submit a file to conduct data matching.



## RECORDS RETENTION SCHEDULE

*Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?*

Yes

*How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.*

GLDS Reimbursables Data Exchange system (Disclosure of Information to Federal State and Local Agencies (DIFSLA), Medicare Part D & B and Taxpayer Address Requests (TAR)) data is approved as temporary, subject to destruction when no longer needed for operational purposes but no longer than 5 years. System owners currently set retention at 1-year. System data is scheduled under several National Archives and Records Administration (NARA) approved disposition authorities: (IMF/IRTF Extracts) Job No. N1-58-09-23, published in IRS Document 12990 under Records Control Schedule (RCS) 18, item 53; (BMF Extracts) Job No. N1-58-09-22,-published in IRS Document 12990 under RCS 18, item 54; and (BRTF Extracts) Job No. N1-58-09-24, published in IRS Document 12990 under RCS 18, item 55.

## SA&A OR ASCA

*Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?*

No

*Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?*

Yes

*Describe the system's audit trail.*

The GLDS Reimbursable Data Exchange system receives tickler (Flat) files from federal, state, and local agencies. These files are logged by the Electronic File Transfer Utility (EFTU) and record counts are monitored to ensure records sent by the agency match what is received by the IRS. These files are then matched via batch processing (no direct access) to the Information Return Master File (IRMF). The IRMF data records are appended to the tickler records provided by the agencies via a batch program and then returned to the respective agencies via EFTU. Record counts are provided for each extract and random files

are quality reviewed for data integrity. Disclosure of Information to Federal, State and Local Agencies (DIFSLA) and IRMF rely on the RACF/GSS-21 IBM Masterfile Platform to capture login information for developer access to their systems. The GLDS Reimbursable Data Exchange system is not responsible for providing data access to individual users. The Office of Governmental Liaison, Disclosure and Safeguards executes and maintains computer matching agreements (CMAs) with agencies participating in the data exchange that outline security/privacy procedures.

## **PRIVACY TESTING**

*Does the system require a System Test Plan?*

No

*Please explain why:*

The GLDS Reimbursables Data Exchange system is a component of the Information Return Master File Research & Support (IRMFRES) system which utilizes the IRMFRES Test Plan (TP), which is a requirement for all testing and may be used as an Enterprise Life Cycle (ELC) functional equivalent for the System Test Plan (STP).

## **SBU DATA USE**

*Does this system use, or plan to use SBU Data in Testing?*

No

## **NUMBER AND CATEGORY OF PII RECORDS**

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

## **CIVIL LIBERTIES**

*Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?*

No

*Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?*

No

*Will this system have the capability to identify, locate, and monitor individuals or groups of people?*

No

*Does computer matching occur?*

Yes

*Does your matching meet the Privacy Act definition of a matching program?*

Yes

*Can the business owner certify that it meets requirements of IRM 11.3.39, Disclosure of Official Information, Computer Matching & Privacy Protection Act?*

Yes

## **ACCOUNTING OF DISCLOSURES**

*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

*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