Date of Approval: **March 11, 2022**

PIA ID Number: **6817**

SYSTEM DESCRIPTION

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

Collection Activity Reports Statutory Reports, CARSR

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?

Collection Activity Reports Statutory Reports, CARSR, MS4B

What is the approval date of the most recent PCLIA?

5/29/2019

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.

Internal Management Governance Board (IMGB)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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.

CARSR is a collection of Tier 1 Legacy platform data extracts, which are executed by the 701 EXEC application that accesses IMF and BMF Masterfile data under Martinsburg Computing Center (MCC) IT-21 GSS Operations. The data from the extracts support the creation of statutory reports, maintained by CARSR, which are used as source documents for preparation of the Pub. 55 - IRS Data Book, and the Excise Tax Trust Fund Certification. These reports also provide tax administration and revenue collection information for W&I, SBSE, CFO, & RAAS.

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:

Interfaces with external entities that require the SSN

Statistical and other research purposes

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

The interfaces for the external entities provide information to the participating agencies for the State Income Tax Levy Program (SITLP) and Municipal Income Tax Levy Program (MITLP). The internal tax processing system Information Returns Processing (IRP) utilizes SSNs for the completion of document matching.

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

The Office of Management and Budget memorandum M-07-16 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The SITLP and MTLP are administered by the CARSR system. The CARSR system requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. This exception also applies to facilitate document matching utilized by the internal tax processing system IRP for these data files which are maintained by CARSR: 1) IMF 1099INT Credit Interest Paid to Taxpayers and, 2) TC530 Recap file (for Currently Not Collectible taxpayers).

Employer Identification Number

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:

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?

No

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.

Corporate File On-Line, Individual Master File (IMF), and Taxpayer Information File are primarily used because they contain the most recent taxpayer transaction codes. The taxpayers name, SSN, and address are needed elements so the state and municipal agencies can perform their matching process, in order to send the IRS the levy funds. The balance due information is needed in order to have the state and municipal agencies levy the proper amount. Secure Data Transport is used to send and receive the data in order to levy the refund and post the levy payment. Posting the levy payment will generate a Case Processing 92, advising of the levy, from the IMF to the taxpayer. CARSR runs extract data for the IRS Government Liaison Data Exchange Program (GLDEP). They disseminate requested and approved portions of the extract data to other federal and state (or city) agencies. The GLDEP was created with the specific intent of sharing federal return and return information with state agencies to assist with state tax administrations. The goals and benefits of the GLDEP is to help the states as follows: to leverage resources, to increase revenue and compliance, and to provide opportunities for enhanced taxpayer outreach and education.

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

All CARSR System Reports and data files, including the data files for SITLP, MTLP, and IRP; are generated by the IRS Enterprise Operations (EOPS) on a pre-determined schedule, then securely stored, maintained, and verified for accuracy with begin and end balancing. These reports and data files are then distributed by EOPS to the various CARSR customers, who in turn verify their applicable reports and related data files for accuracy, timeliness, and completeness.

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 26.019 Taxpayer Delinquent Account Files

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: 3/4/2020
SA&A: Yes
ATO/IATO Date: 11/26/2019

System Name: Business Master File (BMF)
Current PCLIA: Yes
Approval Date: 9/22/2021
SA&A: Yes
ATO/IATO Date: 11/12/2020

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

No

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: Alaska Permanent Fund Dividend (AKPFD)
Transmission Method: EFTU
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?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Information Returns Processing (IRP)
Current PCLIA: Yes
Approval Date: 3/16/2020
SA&A: Yes
ATO/IATO Date: 9/22/2019

System Name: Notice Prints Processing (NPP)
Current PCLIA: Yes
Approval Date: 4/13/2021
SA&A: Yes
ATO/IATO Date: 11/12/2019

Identify the authority.

IRS 6103. In order for the IRS systems: 1) NPP to identify the correct taxpayer to receive the 1099INT mailout form and, 2) IRP to identify taxpayers in Currently Not Collectible status; the taxpayers SSN, name, address, and federal tax liability information is needed by the program/system.

For what purpose?

For: 1) NPP to identify the correct taxpayer to receive the 1099INT mailout form and, 2) IRP to identify taxpayers in Currently Not Collectible status, prior to initiating federal tax administration for taxpayers identified as tax delinquent.

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

No

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: Alaska Permanent Fund Dividend (AKPFD)
Transmission Method: EFTU
ISA/MOU: Yes

Organization Name: Regional Income Tax Agency (RITA)
Transmission Method: EFTU
ISA/MOU: Yes

Identify the authority.

IRS 6103. In order for the participating municipal (RITA) and state (AKPFD) agencies to conduct their levy matching process, the taxpayers SSN, name, address, and federal tax liability information is needed by the program/system.

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

The CARSR system disseminates requested and approved portions of extracted data to Federal IRS Systems, and State (or Municipal) agencies.

For what purpose?

Participating municipal and state taxing agencies are required to match on the SSN, name control and name before deducting the money from the taxpayer's state income tax refund. The federal liability information is need by the municipal and state agencies so the payments can be applied to the correct taxpayer's account. The CARSR system disseminates requested and approved portions of extracted data to approved state or city agencies. This process enables the IRS to collect millions of dollars in delinquent taxpayer revenue.

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?

CARSR extracts data files from IMF and BMF. The CARSR area does not manipulate data or interact with individuals data directly. "Notice, consent, and due process" are provided via BMF, IMF, and its related tax forms and instructions.

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

No

Why not?

CARSR extracts data files from IMF and BMF. The CARSR area does not manipulate data or interact with individuals data directly. "Notice, consent, and due process" are provided via BMF, IMF, and its related tax forms and instructions.

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

CARSR extracts data files from IMF and BMF. The CARSR area does not manipulate data or interact with individuals data directly. "Notice, consent, and due process" are provided via BMF, IMF, and its related tax forms and instructions.

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

Users: Read Only

Managers: Read Only

Developers: Read Only

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

The users must submit a special request to access the CARSR data, via the Business Entitlement Access Request System (BEARS). The request must be approved by the user's manager before being forwarded to the CARSR business unit (BU). The CARSR BU is responsible for reviewing the request and ensuring the user is added to the appropriate access control list in order for the user to receive proper access to the CARSR data.

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.

The Municipal Tax Levy Program is extracted from the State Income Tax Levy Program data for one state. RCS 19 Item 65-State Income Tax Levy Program (SITLP) System.- Delete/Destroy 10 years after cutoff or when no longer needed for operational purposes, whichever is later. RCS 8 Item 44(a)-IRC Â§6103 Accountings (Form 5466-B or equivalent). Form 5466-B, Multiple Records of Disclosure (or equivalent)-Record Copy - Paper (prepared by Disclosure Offices)-Destroy 5 years after processing year, or 30 days after end of month in which record is converted to an electronic image. RCS 8 Item 52-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 of actions taken. Basic Agreements Files, including documents and information on the coordination of Federal/State Exchange programs and related background materials. a. Record Copy - Paper Destroy paper 3 years after receipt of new or amended agreement, or 30 days after end of month in which the record is converted to an electronic image. SITLP data for Alaska is approved for destruction 10 years after end of processing year or when no longer needed for operational purposes, whichever is later (Job No. N1-58-09-65, approved 11-9-09). These disposition instructions are published in IRS Document 12990 under Records Control Schedule (RCS) 19 for the Enterprise Computing Center - Martinsburg. CARSR is not the official records keeping repository of the extracted information in the system. All information in the system is properly scheduled in its original forms under the General Records Schedule and the RCS of the IRS. Extracted Federal Tax Information is provided to state and local agencies under the authority of IRC 6103d for purposes of state tax administration. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under Internal Revenue Manual 1.15.6. For different data types, there are different retention periods. Retention schedules are documented in the Functional Specification Packages.

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.

This system, located on the GSS-21 Tier 1 Legacy platform, only looks at two elements on the monthly report. They are: 1. the userID and 2. the name of the file that was accessed improperly. That report is generated for GSS-21 by the Resource Access Control Facility (RACF).

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

For MTLP and SITLP, the CARSR area performs the testing. The program testing and validation is performed in a secured environment using quality data to ensure the integrity and privacy accountability of any test inputs and outputs. Limited amounts of data are used to further minimize risk of access to personally identifiable information. This is also true for the data files provided to the IRS Systems NPP and IRP.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Testing is conducted by the CARSR area, test results and documentation is found in the IRS Document Management System, which is located within the documentum (DocIT) repository.

SBU DATA USE

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

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

4/3/2019

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

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