Date of Approval: **March 24, 2021**

PIA ID Number: **5940**

SYSTEM DESCRIPTION

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

Alaska Permanent Fund Dividend Levy Program, AKPFD

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?

Alaska Permanent Fund Dividend Levy Program 3274

What is the approval date of the most recent PCLIA?

4/20/2018

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 Level Management Board

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.

To do enforcement action with the use of Electronic levy on the Alaska Permanent Fund Dividend (AKPFD) issued to the residents of Alaska. Alaska sends a data file electronically thru Secure Data Transfer (SDT). We match the AKPFD Applicants with the Unpaid Assessments Accounts (UAA) from Master File (MF) to issue levies against those individuals that owe federal taxes. After the levy is served, Alaska then sends the payments electronically thru Electronic Funds Transfer Program (EFTPS).

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:

Security Background Investigations

Interfaces with external entities that require the SSN

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Delivery of governmental benefits, privileges, and services

Law enforcement and intelligence purposes

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

The AKPFD system requires the use of SSN's 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. In order for the correct tax records to be matched with the Alaska Permanent Fund Dividend database IRS has to be able to make the match using the SSN first, then other identifying characters.

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

None. The Office of Management and Budget Circular A-130 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 AKPFD requires the use of SSN's 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. The PFDD Applicant File is verified against IMF, BMF, CFOL, and TIF for accuracy. The SSN, Name, and Date of Birth must match for the record to be complete and available for inclusion in the program.

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:

Tax Account Information
Name
Mailing address
Phone Numbers
Date of Birth

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:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

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.

The SSN, Name, and Date of Birth must match for the record to be complete and available for inclusion in the program.

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

SSN, Name Control and Date of Birth have to be verified as correct thru SSA's Debtor Match (DM1) Validation once they are, they are then forwarded for matching with both Individual Master File (IMF) and Business Master File (BMF) Unpaid Balance of Assessments meeting AKPFD Levy Requirements in IRM 5.19.9.4.

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: 9/22/2019

System Name: Business Master File (BMF)
Current PCLIA: Yes
Approval Date: 8/27/2018
SA&A: Yes
ATO/IATO Date: 11/12/2019

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 Department of Revenue
Transmission Method: SDT
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?

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 Department of Revenue
Transmission Method: Secure Data Transport (SDT)
ISA/MOU: Yes

Identify the authority.

Transmission of Electronic Levy

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

The Collection Activity and Statutory Reports (CARSR) system disseminates requested and approved portions of extracted data to other Federal and State agencies.

For what purpose?

IRS required to match on the SSN, name control and DOB before matching and issuing a levy on the taxpayer's Permanent Fund Dividend. The federal liability information is need by Alaska so the payments can be applied to the correct taxpayer's account. The CARSR system disseminates requested and approved portions of extracted data to other federal, 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 individual's data directly. "Notice, consent, and due process" are provided via Business Mater File (BMF), Individual Master File (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 individual’s 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 individual’s 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 Online 5081. 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.

Per GRS 4.2, item 130, the PII records are destroyed when no longer needed which is after 400 days.

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.

Access to system files are only granted via RACF (Resource Access Control Facility) on the IBM mainframe. A monthly RACF audit log report is generated identifying all users that have attempted to access system files.

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)?

Testing is conducted by the CARSR area, test results and documentation is found in the IRS Document Management System.

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?

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.

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: Under 50,000

Contractors: Under 5,000

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?

No

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?

No