Date of Approval: **September 09, 2022**

PIA ID Number: **7131**

SYSTEM DESCRIPTION

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

Modernize online payment plan, MOPP

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?

Online Account, OLA,4B

What is the approval date of the most recent PCLIA?

6/16/2021

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Significant System Management Changes

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.

Web Applications (WebApps) Governance Board and Strategic Development Executive Steering Committee. This artifact update is for the Integrated Readiness Review.

Current ELC (Enterprise Life Cycle) Milestones:

Detailed Design/Milestone 4A

System Development/Milestone 4B

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

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

Yes

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.

Online Payment Plan (OPP) will allow taxpayers to determine eligibility to apply for, establish, and revise a payment plan, including an installment agreement, through their account, within OLA. Online Payment Plan(OPP) will: Allow individual taxpayers to establish a payment plan (including installment agreements) Allow individual taxpayers to revise existing payment plans (including installment agreements) and direct debit installment agreements Allow taxpayers with a pre-assessed balance to proactively establish an installment agreement for the current tax year and unassessed balances Provide customized messaging for taxpayers who have either failed or passed plan-specific eligibility checks Allow taxpayers to see their current status related to Installment Agreements (IA), including active long-term, short-term, default, and no IA Within the OLA platform, Online Payment Plan allows taxpayers to self-service their tax liabilities, which has numerous benefits: Reduction in taxpayer calls to the Customer Service Reps (Collection System call volume) Reduction in Information Technology (IT) operating costs by: - Aligning the user experience across channels - Improving the payment plan (including Installment Agreement) functionality - Being more powerful, flexible and improving on limitations in the current system Increased taxpayer compliance Increased tracking of customer use of online payment agreements that can be used to identify additional opportunities to increase taxpayer use of this resource The installment agreement is granted under the authority of IRC code which mandates that taxpayers receive a written confirmation letter. OPP will follow established protocol, in which a failed letter transaction is captured and manually issued by an assigned IRS employee. As such, a letter error handling process was designed, which will capture any failed letter transaction and assigned employees will resolve the letter error. In addition, Installment Agreements established by direct debit, paid through automatic bank withdraws have specific retention requirements per National Automated Clearing House Association (NACHA).

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

Statistical and other research purposes

Other Taxpayer 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
Protection Personal Identification Numbers (IP PIN)
Financial Account Numbers
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:

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

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.

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.

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

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)

PII about individuals for Bank Secrecy Act compliance 31 USC

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.

Online Payment Plan obtains SBU/PII to establish a payment plan or installment agreement. OPP secures taxpayer information from databases IDRS (Integrated Data Retrieval System) and CFOL (Corporate Files Online), including social security number (SSN) and tax account information. Taxpayers are prompted to identify a tax payment plan and amount, as well as the method of payment. When Direct Debit Installment Agreements are requested as a method of payment, taxpayers must enter bank information (routing and account numbers) and SSNs, as per paper and business processes. Entered SSNs are verified by on-screen and backend verifications. If SSN isn't entered, system will show "SSN is required" error. If entered SSN fails to validate against OLA SSN for taxpayers, system will show "Invalid SSN. Check your SSN and try again" error. When Letter error handling: SBU/PII will be captured only in the event of a failed letter transaction. Only the SBU/PII needed to reissue an IA confirmation letter will be captured, which includes SSN as the primary mechanism for identification of the taxpayer. Other SBU/PII will include details regarding the installment agreement needed to reissue the IA confirmation letter including the date of the transaction, the specific tax periods included in the agreement, the payment amount, payment date, and user fee. This information will be captured on a secured storage location, maintained solely by the business owner. The business owner will delegate access to

Customer Service Representative (CSR) leads, who will the pull the data to distribute to employees assigned to resolve the failed letter transactions. Failed letter transactions are worked by designated employees at three campuses and must be processed within 5 working days. Once the IA confirmation letter has been generated, the listing will be deleted from the storage location. For Online Payment Plans- Direct Debit Installment Agreement (DDIA)retention, the IRS is required to retain a record of the taxpayer's authorization for direct debit payments. Per the current IRS records control schedule, direct debit installment agreements must be retained for 12 years. A record of the transaction, to include the required elements: First Name, Last Name and Social Security Number, Amount of transaction, day of monthly payment, Routing number Account Number Bank Customer Name, taxpayer signature and date, must be stored internally for 12 years. Per the Records Information Management, electronic record will not be transferred to federal records but will be stored internally. Reference: Document 12990 (Rev. 11-2017) (irs.gov) Direct Debit Installment Agreements (Form 433 Series) and related documents. These records are used by Compliance function taxpayer contact personnel to set up an agreement between the IRS and the taxpayer. The completed form permits the taxpayer to pay delinquent taxes through installment payments. AUTHORIZED DISPOSITION Retire every 60 days or when no longer needed, whichever is earlier. Destroy immediately after 12 years.

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

All taxpayers are authenticated by Secure Access Digital Identity (SADI) service when logging into OLA to validate their identity and other PII information is accurate prior to authorizing actions within OLA. When an individual sets up a payment plan, Taxpayer PII information and Payment Plan data is populated in Web Apps from authoritative IRS source systems (e.g., IDRS). Additionally, the Taxpayer is presented with their information to review and correct if it is not accurate. Any PII/SBU information provided by the Taxpayer during the plan creation is validated against IRS source systems for accuracy and completeness. Once a payment plan is created, the data is not modified as it is written to Web Apps databases/file systems prior to being securely transmitted to external systems (For example, EDP for Direct Debit Installment Agreement logs or Secure Network Drive for Letter Error Transactions).

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 00.001 Correspondence Files and Correspondence Control Files

IRS 22.062 Electronic Filing Records

IRS 37.006 Correspondence, Miscellaneous Records, and Information Management Records

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 22.061 Information Return Master File

IRS 26.019 Taxpayer Delinquent Account Files

IRS 26.020 Taxpayer Delinquency Investigation 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: SADI (Secure Access Digital Identity)
Current PCLIA: Yes
Approval Date: 7/10/2018
SA&A: Yes
ATO/IATO Date: 10/24/2019

System Name: Web Applications
Current PCLIA: Yes
Approval Date: 8/7/2018
SA&A: No

System Name: Standardized IDRS Access
Current PCLIA: Yes
Approval Date: 2/27/2018
SA&A: No

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)?

No

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: eAuthentication(eAuth)
Current PCLIA: Yes
Approval Date: 7/10/2018
SA&A: Yes
ATO/IATO Date: 10/24/2017

System Name: Web Application Platform Environment
Current PCLIA: Yes
Approval Date: 8/7/2018
SA&A: No

System Name: Standardize IDRS Access
Current PCLIA: Yes
Approval Date: 2/27/2018
SA&A: No

Identify the authority.

IRC Sections 6001, 6011, 6012e(a) - process taxpayer information. IRC Section 6109 - collecting SSN information cyber security compliance

For what purpose?

When online payment plans are created, the information is sent to IDRS for posting to IRS authoritative systems. DDIA authorizations are transmitted to Electronic Data Processing (EDP) for the purpose of retaining payment plans for 12 years in order to comply with legal obligations. The letter error transactions are transmitted to the shared drive environment for the purpose of Customer Service Representatives manually initiating payment plan confirmation letters to be sent to taxpayers.

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

No

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

No

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?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Yes

When was the e-RA completed?

4/22/2019

What was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity
Confidence based on Single Factor Identity Validation

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?

The individual is informed during the online set up process regarding notice and consent. The information needed to establish the payment plan or installment agreement is mandatory and solely utilized to establish the payment plan or installment agreement. Failure to provide the information needed to establish the payment plan or installment agreement will not allow the transaction to be completed.

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):

Individuals consent to providing the information needed to establish the payment plan or installment agreement and to the specific use of the information by check box acceptance during the final step of plan creation. The consent is captured through back-end processing.

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

The taxpayer has due process by writing, calling, faxing, or visiting the IRS. They are also provided due tax forms 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

System Administrators: Administrator

Developers: Read Only

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Only

Contractor System Administrators: Administrator

Contractor Developers: Read Only

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

For both letter error handling and EDP DDIA retention, access to the storage system would be maintained by the business owner. For letter error handling, the business owner would grant read only access to assigned team leads, to retrieve the list of failed letter transactions.

The leads would then assign the cases to employees to work the letter failure. The listing would be cleared after the letter issued. The letter error handling process will follow established procedures as identified in IRM 5.19. 1, which requires that the letter errors be processed within 5 working days of receipt. For EDP DDIA retention, per NACHA requirements, all DDIA transactions are required to be maintained for 12 years. The business owner would maintain control and be solely responsible to research these logs.

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.

Online Payment Plan, Letter Error Handling and EDP DDIA Records Retention adhere to established guidelines found in Document 12990 (Rev. 11-2017) (irs.gov) RCS 28 Item 158- Online Payment Agreement (OPA). The Online Payment Agreement (OPA) is an Integrated Customer Communications Environment (ICCE) Web Applications (Web Apps) applet that allows approved taxpayers to conduct payment agreement activities on-line. (Job No. N1-058-11-11) For Online Payment Plan: Taxpayer input data would be deleted once the successful transaction has occurred. AUTHORIZED DISPOSITION Delete/Destroy any (taxpayer-entered) cached input files and data immediately following validation of receipt by the system. The data repositories and warehouses of all other source data are appropriately scheduled under other Records Control Schedules of the Internal Revenue Service. For letter error handling: Once the letter issuance has been manually processed, the record would be deleted. AUTHORIZED DISPOSITION Delete after successful entry and capture by the Individual Master File System, which is appropriately scheduled under RCS 29. Item 69(5) For EDP DDIA Records Retention: Direct Debit Installment Agreements (Form 433 Series) and related documents. These records are used by Compliance function taxpayer contact personnel to set up an agreement between the IRS and the taxpayer. The completed form permits the taxpayer to pay delinquent taxes through installment payments. AUTHORIZED DISPOSITION Destroy immediately after 12 years.

SA&A OR ASCA

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

Yes

What date was it completed?

12/2/2021

Describe the system's audit trail.

MOPP adheres to the following process for maintaining an audit trail of the system. This policy applies to both Letter Error Handling and DDIA Authorization Log Retention: An Audit Plan has been created for this system (OLA) by the project team with the support of Enterprise Security Audit Trail (ESAT)/Security Audit and Analysis System (SAAS). The system collects legal events for Treasury Inspector General for Tax Administration (TIGTA), Criminal Investigation (CI), and the CSDW to establish chain of custody for each transaction within all applications to be used as evidence and prove audit trails. It records all actions of the taxpayer/user in near-real-time and transmits to ESAT/SAAS logs for Cybersecurity review. The audit trail contains the audit trail elements as required in current IRM 10.8.3, Audit Logging Security Standards. The system audit trail was a systemic account of the processes and data management on Web Apps directory and database. AUDIT will be enabled for SELECT, INSERT, UPDATE and DELETE operation on DB table to ensure all data operations are audited and Audit will be enabled on the folder on WAES server (RHEL) that will store the files containing failed Letter transactions and DDIA authorization logs.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

Test Strategy Implementation Plan (TSIP) is used in place of a 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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

By using taxpayer supplied PII and IP Addresses, the IRS will have the capability to identify, locate, and monitor taxpayers. The primary purpose of doing this is to correlate website usage with other IRS processes. For example, tracking notice response rates.

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?

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