Date of Approval: **August 18, 2021**

PIA ID Number: **6371**

**SYSTEM DESCRIPTION**

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

Order A Transcript (by mail), OAT

**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?*

Order A Transcript (by mail), OAT #3330

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

7/10/2018

*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.*

SBSE Governance 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.

Order A Transcript (OAT) is accessed from the IRS.Gov webpage. OAT is used by the public to order copies of Account and/or Return transcripts - Users authenticate by entering information directly into the online template. Orders are fulfilled via mail to the user's address of record - Due process for any errors in transcript information is available pursuant to Title 26 USC.

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:

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

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

This application does truncate the Social Security Number (last four digits are masked).

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

This application does truncate the Social Security Number (last four digits are masked). The application cannot mitigate the use of Social Security numbers until an alternate identifier has been adopted by the IRS to identify taxpayers.
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
- Date of Birth
- 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:

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.

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.

Authenticate User Identity and verify transcript is available prior to allowing order. OAT is not a database. Data entered by the user is not retrievable once it is submitted.

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

The validation process verifies the accuracy and completeness of the information input by the taxpayer in accordance with the business rules. It is worth noting that the only validation OAT performs is a validation of the taxpayer's SSN, TIN type, File Source Code, Date of Birth, Street Address and Zip Code against IRS records in the National Account Profile (NAP) to authenticate the applicant. OAT passes the TIN entered by the taxpayer to NAP. If the information matches IRS records, the request process will proceed. If the information does not match IRS records, the record will reject back to the taxpayer for correction and re-submission. If the taxpayer cannot correct the information within three attempts, he/she will be given an error page and their session will end.

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 System
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: Security Audit and Analysis
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 6/12/2017

System Name: National Account Profile
Current PCLIA: Yes
Approval Date: 2/27/2020
SA&A: Yes
ATO/IATO Date: 2/9/2021

System Name: Transcript Delivery System
Current PCLIA: Yes
Approval Date: 8/7/2019
SA&A: Yes
ATO/IATO Date: 3/1/2021

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: National Account Profile (NAP)
Current PCLIA: Yes
Approval Date: 2/27/2020
SA&A: Yes
ATO/IATO Date: 2/1/2021

System Name: Application Messaging and Data Access Services (AMDAS)
Current PCLIA: No
SA&A: No

Identify the authority.

Federal tax administration

For what purpose?

To support taxpayers in receiving accurate information.

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?

2/1/2021

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?

Notice is provided on the instructions for Form 4506 T. Privacy Act and Paperwork Reduction Act Notice. We ask for the information on this form to establish your right to gain access to the requested tax information under the Internal Revenue Code. We need this information to properly identify the tax information and respond to your request. You are not required to request any transcript; if you do request a transcript, sections 6103 and 6109 and their regulations require you to provide this information, including your SSN or EIN. If you do not provide this information, we may not be able to process your request. Providing false or fraudulent information may subject you to penalties.

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):

Taxpayers are not required to order a transcript. They may simply choose not to make use of the system. If they do choose to request a transcript, sections 6103 and 6109 and respective regulations require they provide this information, including a TIN.

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

The Taxpayer Bill of Rights publication 1 outlines the baseline for 'due process' that business follows. Due process is not applicable to the public in general as the system does not "use" the event information to interact with the tax paying public in any way. IRS employees and contractors using IRS email and web services may face disciplinary action for the misuse of SSNs. All IRS employees will be given the opportunity to defend their actions before a final determination is made. Contractor employees will be afforded any rights granted within the regulations that cover the specific contract they are working under. The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.
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 Only

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

Access is determined by business need and is requested via the Online (OL) 5081 system. Employee manager approves based on application need.

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.

All records housed in the OAT system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedule (RCS) 29, Item 183 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.
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?

4/1/2021

Describe the system's audit trail.

OAT audit data is captured by the Security Audit and Analysis System (SAAS). Audit trail logging for the application is sent to SAAS via Application Messaging and Data Access Services (AMDAS) regarding the success or failure of each transaction that reaches the back-end authentication of the user. The SSN, TIN type, File SourceCode, Date of Birth, Street Address and Zip Code are extracted from the National Account Profile (NAP) on a Read Only basis. The information entered by the user is captured for audit trail purposes. These Audit trails are for internal use and are closely guarded. They are only available to IRS employees who follow the proper procedures to gain access to them, which is by going through the OL5081 process. A manager must approve the OL5081 request and then an administrator will grant the access if the person is authorized by the organization to view the reports.

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)?

The Integrated Customer Communications Environment (ICCE) System Test Plan document is developed for the use by ICCE project team. It is a configuration item and is stored in DocIT (technical documentation system). Suggested modifications to the document are submitted in writing to the Systems Support Section. Documents are stored and distributed through DocIT in the System Test Plan (STP) folder under the Test Plans and Test Reports parent folder.
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?

OAT complies with the requirements of IRM 10.8.1.3.4.6 in regards to developer security testing. This means that a work request (WR) or change request (CR) must be in place before a piece of code can be associated with it. Once development is completed the code is then checked back in for testing. There is a team staffed to accomplish independent testing before the code is promoted to production. A final review is accomplished by an in-house staff leader. WR/CR tickets can be Knowledge Incident/Problem Service Asset Management tickets related to production issues; they can be issues discovered during testing; or they can be user change requests.

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: Under 50,000

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?

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