Date of Approval: July 10, 2018 PIA ID Number: **3330**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Order A Transcript (by mail), OAT

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Short Term Transcript (ST-TRA) , PIAMS # 897

Next, enter the **date** of the most recent PIA. 05/22/2015

Indicate which of the following changes occurred to require this update (check all that apply).

No	Addition of PII
No	Conversions
No	Anonymous to Non-Anonymous
No	Significant System Management Changes
No	Significant Merging with Another System
No	New Access by IRS employees or Members of the Public
No	Addition of Commercial Data / Sources
No	New Interagency Use
No	Internal Flow or Collection

Were there other system changes not listed above? Yes

If yes, explain what changes were made. The capability to order Form 4506 has been removed.

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
No	System Development/Milestone 4B
No	System Deployment/Milestone 5
Yes	Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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.

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.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **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

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes	On Primary	Yes	On Spouse	No	On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
No	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Practitioner Tax Identification Number (PTIN)

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

The OAT 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.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

On Primary	On Spouse	On Dependent	Selected	PII Element
Yes	Name	Yes	Yes	No
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
No	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

Yes	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(
Yes	SSN for tax returns and return information is Internal Revenue Code Section 6109
No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	PII for personnel administration is 5 USC
No	PII about individuals for Bank Secrecy Act compliance 31 USC
No	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

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.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number	SORNS Name
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File
IRS 34.037	IRS Audit Trail and Security Records System

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
National Account Profile	Yes	03/21/2017	Yes	02/09/2017
Transcript Delivery System	Yes	04/20/2018	Yes	02/21/2018
Security Audit and Analysis System	Yes	04/13/2018	Yes	06/12/2017

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agencies? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
National Account Profile (NAP)	Yes	03/21/2017	Yes	02/09/2017

Identify the authority and for what purpose? Federal tax administration.

12b. Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

12e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? Yes

16a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

16a1.If **yes**, when was the **e-RA** conducted? 11/30/2017

If **yes**, what was the approved level of authentication?

Level 2: Some confidence in the asserted identity's validity.

Single Factor Identity Validation

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide 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.

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

18a. If **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.

19. 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.

I. INFORMATION PROTECTION

20. 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

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

IRS Employees? Yes

IRS Employees?	Yes/No	Access Level (Read Only/Read Write/ Administrator)
Users	No	
Managers	No	
Sys. Administrators	Yes	Read and Write
Developers	Yes	Read-Only

Contractor Employees? No

21a. 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.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?

Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and 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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 05/22/2017

23.1 Describe in detail 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 for each transaction that reaches the back-end authentication of the user. The SSN, TIN type, File Source Code, 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process,** 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 regard 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.

24b.1. If **completed**, 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.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Under 50,000
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. Other: No

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804?* No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report