Date of Approval: **August 07, 2019**

PIA ID Number: **4156**

## SYSTEM DESCRIPTION

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

EServices, eServ

*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?*

eServices, 4b 3375

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

4/20/2018

*Changes that occurred to require this update:*

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.*

W&I Division Executive Resources 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?*

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.*

eServices is a suite of web-based products allows tax professionals and financial institutions, state taxing authorities, and government entities to conduct business with the IRS electronically. These services are only available to approved IRS business partners and not available to the general public. eServices is available via the Internet 24 hours a day, 7 days a week. The e-Services software application suite consists of External Systems Authentication Management (ESAM), Transcript Delivery System (TDS) and Tin Identification Number Matching (Tin Matching), each offering a unique set of features and capabilities to support external users and internal users. The addition of the eServices API functionality, eServices is adding API capability to the three eServices applications: TDS, TINM, and SOR to move scripting users to Application Program Interface (API) and facilitate the move of all eService transactions in robot (BOT/SHAPE) mitigation mode. This will strengthen security around eServices applications. There will be no changes to any of the three applications functionalities. The API will provide a very secure channel to external users to access the data.

## 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)

Another compelling reason for collecting the SSN

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

The SSN is used to authenticate. After authentication the user is assigned an EIN or TIN to conduct business. The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. eServices system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

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

The SSN is used to authenticate. After authentication the user is assigned an EIN or TIN to conduct business. The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. eServices system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

Employer Identification Number

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

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Standard Employee Identifier (SEID)

Internet Protocol Address (IP 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 (SBUList)*

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?*

Yes

*Describe the other types of SBU/PII that are applicable to this system.*

Federal Tax Information

*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.*

eServices contains personally identifiable information (PII) such as the name, date of birth, address, and social security number. This type of information is considered privileged and unauthorized disclosure could cause embarrassment to IRS and potential liability concerns for Wage and Investment.

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

Accuracy: Data entered for all e-Services Products is processed and error checked at multiple levels throughout e-Services transactions to ensure accuracy. The successful authentication and authorization of the third-party user of the system provides the first level of data verification entered on behalf of the taxpayer. The second level consists of Internet browser surface editing as the user inputs data for submission to the application. The relevant e-Services server will conduct a third check on user entered data. Finally, the application will match data against the systems to determine validity. Completeness: Data fields required for successful interactive e-Services transactions will undergo checks during online input. The application will not allow the user to submit incomplete requests and will provide them the ability to edit incorrect data prior to final submission. Timeliness: The data received from other IRS systems for the purposes of validation are updated on a daily or weekly basis to ensure that the information entered is current. Once the data is collected and validated, the data is kept as current as the user who provides it.

## 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 34.037 | Audit Trail and Security Records System |
| IRS 22.062 | Electronic Filing Records |
| IRS 22.061 | Individual Return Master File |
| IRS 24.030 | Customer Account Data Engine Individual Master File |
| IRS 24.046 | Customer Account Data Engine Business Master File |
| IRS 37.009 | Enrolled Agent and Enrolled Retirement Plan Agent Records |

## RESPONSIBLE PARTIES

*Identify the individuals for the following system roles:*

## For 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: Data Master (DMI)

Current PCLIA: No

SA&A: No

System Name: Payer Master File (PMF)

Current PCLIA: Yes

Approval Date: 3/9/2017

SA&A: No

System Name: User Interface From Registration

Current PCLIA: No

SA&A: No

System Name: Taxpayer Professional Preparer Tax System (TPPS)

Current PCLIA: Yes

Approval Date: 3/9/2017

SA&A: Yes

ATO/IATO Date: 8/29/2017

System Name: Residual Master File (RTF/RMF)

Current PCLIA: No

SA&A: No

System Name: Business Master File (BMF)

Current PCLIA: Yes

Approval Date: 8/27/2018

SA&A: Yes

ATO/IATO Date: 3/2/2019

System Name: Individual Master File (IMF)

Current PCLIA: Yes

Approval Date: 3/6/2017

SA&A: Yes

ATO/IATO Date: 9/22/2018

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

Yes

*For each federal 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).*

Name: Specifically designated Nationals

Transmission Method: Treasury Download

ISA/MOU: No

Name: Federal Bureau of Investigation Criminal Justice Information System (FBI CJIS)

Transmission Method: Simple Mail Transfer Protocol

ISA/MOU: Yes

Name: General Service Administration System Awards Management (GSA SAM)

Transmission Method: Hypertext Transfer Protocol Secure

ISA/MOU: Yes

*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: Integrated Customer Communications Environment

Current PCLIA: Yes

Approval Date: 4/28/2019

SA&A: Yes

ATO/IATO Date: 6/27/2019

System Name: Secure Object Repository

Current PCLIA: Yes

Approval Date: 5/31/2019

SA&A: Yes

ATO/IATO Date: 12/5/2018

*Identify the authority*

Internal Revenue Code Section 6109

*For what purpose?*

To provide transcripts to individual taxpayers.

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

Yes

*Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).*

Organization Name: The Centers for Medicare & Medicaid Services (CMS)

Transmission Method: Integrated Enterprise Portal Transactional Portal Environment (IEP-TPE)

ISA/MOU No

*Identify the authority*

Publication 2108A

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

Expanded the use of the Bulk TIN Matching application.

*For what purpose?*

Expanded the use of the Bulk TIN Matching application to verify TINs for validating applications for medical services.

*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: State Tax Agencies

Transmission Method: Simple Mail Transmission Protocol (SMTP)

ISA/MOU Yes

*Identify the authority*

Internal Revenue Code 6103(d).

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

A state taxing authority can gain access to Transcript Delivery System (TDS) by completing a Memorandum of Understanding (MOU) and Implementing Agreement that is negotiated and signed by both the state and IRS authorities based upon Internal Revenue Code 6103(d)

*For what purpose?*

A state taxing authority can gain access to Transcript Delivery System (TDS) by completing a Memorandum of Understanding (MOU) and Implementing Agreement that is negotiated and signed by both the state and IRS authorities based upon Internal Revenue Code 6103(d).

*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?*

11/10/2017 12:00:00 AM

*What was the approved level of authentication?*

Level 3: High confidence in the asserted identity's validity

# 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 alerted before submission is complete right when the user clicks the submit button. The "authority" that authorizes the solicitation of the information would generally be the applicable sections of the Internal Revenue Code. Whether disclosure is "mandatory or voluntary" relates to whether the individual is required to provide the information requested or may refuse to do so.

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

No

*Why not?*

The "effects" upon an individual of not providing all or part of the requested information should include a brief statement of any penalties involved; it should advise the individual of incidental effects such as inability to complete their request through eServices.

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

Third Parties can contact the Electronic Products & Services Support help desk if they have issues with information access, correction or redress.

## 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 Write

Managers: Read Write

System Administrators: Read Write

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

IRS employees request access to specific applications on the Employee User Portal (EUP) by submitting an Online 5081 form. Managerial approval is required. The applicant sponsors and oversees its member interactions with IRS e-Services. The applicant sanctions and ensures that its members act in a responsible and appropriate manner when using IRS e-Services. Failure of the applicant to properly execute their security and privacy responsibilities will result in the possible termination of the applicant's access to e-Services and possible legal prosecution.

## RECORDS SCHEDULE

*Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) archivist 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.*

eServices records will be maintained in accordance with Records Control Schedules (RCS) 19, Item 84 and RCS 17, Item 25, as appropriate and in context with a specific subsystem. All subsystem data meeting end of retention period requirements will be eliminated, overwritten, degaussed, and/or destroyed in accordance with National Archives and Records Administration (NARA)-approved disposition authorities for that system's data, and done so in the most appropriate method based upon the type of storage media used.

## 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?*

2/21/2018

*Describe the system's audit trail.*

The system collects the following audit trail data items: Date and time that the event occurred; The unique identifier (e.g., user name) of the user or application initiating the event; Type of event; Subject of the event (e.g., the user, file, or other resource affected) and the action taken on that subject; and the outcome status (success or failure) of the event. Employee and contractor transactions that add, delete, modify, or research a tax filer's record. Employee and contractor transactions that add, delete, modify, or research an employee's record (personnel and financial). Employee and contractor transactions that add, delete, or modify an employee's access to Employee User Portal (EUP), including changes to EUP roles or sub-roles. Furthermore, systems that store or process taxpayer information includes the following data elements, where applicable: The type of event (e.g., command code) The terminal and employee identification Date and time of input Account accessed to include the TIN, master file tax (MFT), and tax period.

## 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)?*

Test results are stored in DocIT, a web-based electronic document management system powered by the enterprise standard tool Documentum. This is a tool that provides documentation control for IT projects.

*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?*

eServices is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

## 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: Under 5,000

Members of the Public: 100,000 to 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?*

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