Date of Approval: April 20, 2018 PIA ID Number: **3375**

A. SYSTEM DESCRIPTION

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

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.

eServices – PIAMS # 3307

Next, enter the **date** of the most recent PIA. 3/16/2018

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
Yes	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? No

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.

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.

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 No 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)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	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 SSN is used to authenticate. After authentication, the user is assigned an EIN or TIN to conduct business.

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.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	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.
Yes	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
No	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(a)
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.

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.

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

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.

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
Treasury/IRS 00.001	Correspondence Files and Correspondence Control Files
Treasury/IRS 34.037	IRS Audit Trail and Security Records System
Treasury/IRS 22.062	Electronic Filing Records
Treasury/IRS 22.061	Information Return Master File
Treasury/IRS 24.030	Customer Account Data Engine Individual Master File
Treasury/IRS 24.046	Customer Account Data Engine Business Master File
Treasury/IRS 37.009	Enrolled Agent and Enrolled Retirement Plan Agent Records

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 PIA?	PIA Approval Date	SA & A?	Authorization Date
Data Master (DM1)	No		No	
Payer Master File (PMF)	Yes	03/12/2014	Yes	12/04/2015
User Interface from Registration	No		No	12/04/2015
Taxpayer Professional Preparer Tax System (TPPS)	Yes	01/18/2013	Yes	03/29/2017
Individual Master File (IMF)	Yes	05/05/2014	Yes	11/06/2017
Residual Master File (RTF/RMF)	Yes	05/28/2014	No	11/06/2017
Business Master File (BMF)	Yes	08/17/2015	Yes	02/02/2017

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

If **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).

Organization Name	Transmission method	ISA/MOU
Specifically designated Nationals	Treasury Download	No
Federal Bureau of Investigation Criminal Justice Information System (FBI CJIS)	Simple Mail Transfer Protocol	Yes
General Service Administration System Awards Management (GSA SAM)	Hypertext Transfer Protocol Secure	Yes

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 PIA?	PIA Approval Date	SA & A?	Authorization Date
Integrated Customer Communications Environment	Yes	06/01/2016	Yes	07/01/2017
Secure Object Repository	Yes	09/05/2015	No	07/01/2017

Identify the authority and for what purpose? To provide transcripts to individual taxpayers (Internal Revenue Code Section 6109).

12b. Does this system disseminate SBU/PII to other Federal agencies? Yes

If **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	Transmission method	ISA/MOU
The Centers for Medicare & Medicaid Services (CMS)	Integrated Enterprise Portal Transactional Portal Environment (IEP-TPE)	No

Identify the authority and for what purpose? Expanded the use of the Bulk TIN Matching application to verify TINs for validating applications for medical services (Publication 2108A).

12c. Does this system disseminate SBU/PII to State and local agencies? Yes

If **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	Transmission method	ISA/MOU
State Tax Agencies	Simple Mail Transmission Protocol (SMTP)	Yes

Identify the authority and 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).

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

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? 11/10/2017

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

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

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?
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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If 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.

19. 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.

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	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Read-Only
Developers	No	

Contractor Employees? No

21a. 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.

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? No

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.

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.

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? 2/21/2018

23.1 Describe in detail 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.

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?
e-Services continuous monitoring testing was conducted on February 28, 2014. All documents have been updated.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? Documents are stored in Docit.

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: 5,000 to 10,000
26c. Members of the Public: 100,000 to 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? Yes

If **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

End of Report