

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. eAuthentication, eAuth
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.
eAuthentication (eAuth), 289, MS3/4A during Release 2.0

Next, enter the **date** of the most recent PIA. 1/29/2013

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
Yes Internal Flow or Collection

Were there other system changes not listed above? Yes

If yes, explain what changes were made. Use of PII data in Fraud Analysis

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
Yes 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.

The objective of the eAuth project is to provide a core centralized security mechanism that integrates with the IRS infrastructure. This document outlines the components that constitute eAuthentication. The eAuth project will not be building end-user applications, but will provide a framework for identity-proofing and establishment of identities through credentialing in accordance with NIST SP 800-63 requirements thereby providing security to the applications it protects at multiple levels of assurance. The following enhancements and capabilities are included in the eAuth R2.x release: • Implementation of IRS Levels of Assurance (LoAs): o NIST 800-63 Level 1 • IRS Level of Assurance B – Un-proofed o NIST 800-63 Level 2 • Level of Assurance C – Proofed against IRS data sources (already implemented in eAuth R1) • Level of Assurance D - Proofed against IRS data sources and third party Knowledge Based Authentication (KBA) • Level of Assurance E - Proofed against IRS data sources and third party financial account verification o NIST 800-63 Level 3 • Level of Assurance F - Proofed against IRS data sources, financial account verification, address of record non-repudiation • Facilities for user registration and authentication for each of these Levels of Assurances (LoAs) • Multi-factor authentication credential issuance per NIST 800-63 Level 3, and credential lifecycle management for users proofed to LoA F

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 Yes 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).

SSNs are only utilized when required (i.e. to enable the ID proofing service). For this reason, eliminating the use of SSNs is not applicable to eAuthentication.

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.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No

Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
Yes	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
Yes	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
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

6d. Are there other types of SBU/PII used in the system? Yes

If yes, describe the other types of SBU/PII that are applicable to this system. Challenge Question and Answer User ID and Password Phone Number Email Address Secondary email address IP Address IP PIN Device ID SEID Financial Account Information Home Equity Loan Number Auto Loan Number Mortgage Loan Number

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

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>Yes</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	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.

PII data collected by the eAuthentication is used to validate and authenticate individuals trying to access IRS services via internet. The information is required to ensure only valid and approved IRS taxpayers and Non-Filers may access IRS services. The FOIA and Privacy Act requests require identity proofing an individual. IRM 11.3.2.3.2 states current requirements for external authentication of users to IRS systems. It requires use of identity proofing elements such as taxpayer name, taxpayer address, taxpayer Social Security number and taxpayer date of birth and/or filing status. The other business use of the collected PII information is to conduct fraud analysis to identify and deter fraudulent usage of eAuth system by unauthorized users

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

PII is submitted directly by the taxpayers and tax preparers. Once the user inputs their PII data, it gets validated against the IRS internal data source ICCE (validating they are who they say they are) .If the information is not available for the users (Non-Filers) their PII data is validated against third party(Equifax) data providers . Drop down menus and syntax requirements are enforced throughout the application to ensure the accuracy and completeness of data input.

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 24.030 CADE Individual Master File

Treasury/IRS 24.046 CADE Business Master File

Treasury/IRS 34.037 IRS Audit Trail and Security 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. N/A

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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Prisoner File from W&I	No		No	
Return Review Program (RRP)	Yes	01/23/2015	No	
ID Theft File (IMF)	Yes	05/02/2014	No	
Office of Compliance and Analytics (OCA)	No	05/02/2014	No	

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 agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
Equifax	In the case of Non-Filers Identity proofing, eAuth receives the standardized address back from Equifax after successful verification	Yes
IRS is entering in a multi-vendor data services contract and the specific vendor can change from the current vendor in use	TBD	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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
ICCE	No		No	

Identify the authority and for what purpose? ICCE for Identity Proofing.

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

12e. Does this system disseminate SBU/PII to other Sources? Yes

If **yes**, identify the other source(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**

Equifax Secured channel via HTTPS Yes

Identify the authority and for what purpose? Third party sources - Approved 3rd party data providers and approved 3rd party service providers. There is an ISA & MOU with Equifax.

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, 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

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

Level 1: Little or no 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?

Notice is provided on the IRS.GOV. Due process is provided pursuant to 5 USC.

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): Individuals can opt not to proceed with the online session. There is an alternative process available at the IRS to obtain the service the user is looking for. Due process is provided pursuant to 5 USC.

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

The system will allow affected 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

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

Contractor Employees? Yes

<u>Contractor Employees?</u>	Yes/No	Access Level	Background Invest.
Contractor Users	Yes	Read and Write	Moderate
Contractor Managers	Yes	Read and Write	Moderate
Contractor Sys. Admin.	No		
Contractor Developers	Yes	Read and Write	Moderate

21a. How is access to SBU/PII determined and by whom? Taxpayers who chose to utilize eAuthentication services and register with the system have write access to their own user profile only. eAuth system administration is performed by IRS Enterprise Operations (EOps) group and IRS W&I EPSS. eAuth administration will be performed by IRS employees and/or contractors whose access to eAuth system is granted via the Online 5081 process.

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.

The National Archives and Records Administration (NARA) approved the destruction of eAuthentication data (user profiles) 7 years, 6 months after account expiration (Job

No. N1-58-12-6, approved 11/14/2012). These disposition instructions will be published in Records Control Schedule 17 for Information Technology (IRS Document 12990), Item 31 when next updated. As required under the IRS Enterprise Architecture, a plan will be developed to purge the eAuthentication datastore (or records repository) of records eligible for destruction in accordance with the Records Control Schedule, as well as IRS records management requirements in IRMs 1.15.3 (Disposing of Records) and 1.15.6 (Managing Electronic Records).

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)? In-process

23a. If **yes**, what date was it completed?

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion? 10/13/2015

23.1 Describe in detail the system's audit trail. PII information collected by eAuth is sent to Integrated Customer Communications Environment (ICCE) system for Identity Verification. Auditing events of ICCE system is outside of eAuth boundary. eAuth is generating log files that are sent to the Security-1 Security Audit and Analysis System (SAAS) for handling and audit review. The following elements are collected: - taxpayer, non-filers and IRS employee (security, system and database administrator) login (user ID and passwords used to login) taxpayer, non-filers and IRS employee (security, system and database administrator) logoff -taxpayer, non-filers and IRS employee (security, system and database administrator) change of password - Creation and/or modification of user accounts by users during the Registration and Update Profile processes - Resetting users passwords using challenge questions and answers - IRS system and database administrators running or switching system and/or privileged accounts - Clearing of audit files (system accounts) - Start up and shut down of audit functions (system accounts) - Business application utilized to retrieve taxpayer's SSN using a taxpayer user ID - Change of file and/or user permissions - Batch files made to an application (i.e. batch file updates for date of death; ID Theft flag; deletion of a taxpayer account; and the insertion of restricted TINs that are unable to create an account) - Application critical record changes - All ID proofing services, creating a profile, and updating a profile - Negative TIN service request to the MITS-18 Enterprise Application Integration Broker (EAIB) to check administrator access to taxpayer data - All system and database administrator actions -Changes to database tables and/or application records The following fields are captured in audit logs with the corresponding events where applicable: first name, last name, SSN, DOB, Filing Status and Address used to ID proof taxpayers and Non-filers. These Auditing events are updated in eAuth.

J. PRIVACY TESTING

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

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

If **in process**, when is the test plan scheduled for completion? 1/29/2016

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: Under 5,000
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
