NOTE: The following reflects the information entered in the PIAMS Website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: 04/15/2014 PIA ID Number: **820**

1. What type of system is this? New

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

eAuth Data Extract ,

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	Over 1,000,000

4. Responsible Parties:

N/A

5. General Business Purpose of System

IRS is seeking to expand its online service delivery while simultaneously taking steps to proactively deter identity theft. To meet these goals IRS has implemented an eAuthentication (eAuth) product that allows taxpayers to validate their identity and create an online account to access two other products, IP PIN and Get Transcript. This PIA relates to the analysis of a data extract of multiple daily reconciliation files sent by Equifax for eAuthentication (eAuth) data and eAuth account usage data provided by Cybersecurity. The purpose of the analysis of the data extract is to assess the accuracy of the authentication product (using the results of the knowledge based authentication) and to detect potentially fraudulent behavior after the point of authentication (using the eAuth account usage data). The results of the analysis will inform improvements to the authentication product configuration as well as help detect any account compromise after authentication. The data will also be used in a cross-channel analysis of all relevant authentication techniques (eAuth, CSR-OOW (call-in channel for those in the Taxpayer Protection Program (TPP) to authenticate over the phone), eOOW (for those in the TPP population to authenticate online), walk-ins to the Taxpayer Assistance Centers (TACs). This cross-channel analysis will allow IRS to have a holistic understanding of the accuracy of all authentication techniques enabling both near / long term improvements in authentication accuracy as well as the detection / mitigation of potentially fraudulent account access. Due process is provided pursuant to title 26.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) No

6a. If Yes, please indicate the date the latest PIA was approved:

6b. If Yes, please indicate which of the following changes occurred to require this update.

- **System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes)**
- **System is undergoing Security Assessment and Authorization**

6c. State any changes that have occurred to the system since the last PIA

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	Yes	
Employees/Personnel/HR Systems	No	
		Other Source:
Other	No	

---

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
spouse name	Yes	No
IP Address	Yes	No

10a. Briefly describe the PII available in the system referred to in question 10 above.

Reconciliation Files Data: The PII includes data from KBA questions; some of the data in the question is associated with the taxpayer identity and some is false (i.e., to generate the question choices). Some of the questions are simulated and contain no information associated with the taxpayer identity. Account Usage Data: For user created accounts, this will include data on the user generated user account name, email, and password as well as the date and time of any log in activity to the eAuth applications. It will also include data on the application accessed (IP PIN or Get Transcript), and, if applicable, the type of transcript requested, the year of the transcript. Data Collection Instrument (DCI) data from Accounts Management (AM) Customer Service Representative (CSR) based High Risk Authentication (HRA) process and from Field Assistance's in-person authentication processes executed at Taxpayer Assistance Centers (TACs). Responses of callers and walk-ins seeking identity authentication would be captured in a DCI and then sent via encrypted email to a secure email inbox that is access-controlled. Data from inbox is stored on an access-control folder in Thor (CDW's user server).

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

IRC 6109 - provision authorizing IRS to use SSNs for tax identification purposes

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

There is no possible alternative. The SSN is input by the user to authenticate their identity and create an account through eAuth. The SSN is needed to link the account information with other tax data (such as return level data) to help identity possible identity thieves passing the KBA authentication techniques and to analyze the account application access to identify unusual patterns that could indicate fraudulent activity.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

None

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Cybersecurity maintains an audit trail of access to eAuth account usage databases and eAuth Equifax reconciliation files (via 5081), and then provides OCA with an extract. OCA users will place the data extract on a folder in CDW and restrict read/write access to the folder to IRS analysts and contractors working on the specific eAuth identity authentication initiative. [NOTE: the vendor may also at any time surmount current technical constraints to enable secure online account-based access to the reconciliation file.]

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If Yes, the system(s) are listed below:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
	No		No	

b. Other federal agency or agencies: No

If Yes, please list the agency (or agencies) below:

c. State and local agency or agencies: No

If Yes, please list the agency (or agencies) below:

d. Third party sources: Yes

If yes, the third party sources that were used are:

Equifax KBA quiz data for eAuth authentication technique (contained in reconciliation reports)

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): No

g. Other: No **If Yes*, specify*:**

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

This PIA does not cover new collection of PII. The PII is collected through other existing systems. This PIA covers storage and analysis of a data extract from those existing systems. The Office of Compliance Analytics (OCA) is working with W&I and RICS to identify risks associated with online identity authentication and online user account

creation. In order to continue to protect identities, IRS continually assess the how well the Service has safeguarded users of the authentication methods throughout their entire interaction with the IRS, from authentication through account creation to application access. OCA will analyze the Equifax reconciliation reports (KBA outcomes) to ensure that when an identity is asserted that the KBA is capable of distinguishing real taxpayers from identity thieves. Another potential risk is identity theft after the point of creation of eAuth accounts. Once an eAuth account is created, users can further access IP PINs and request a transcript, both of which can be used by identity thieves for filing fraudulent tax returns. OCA will use eAuth user account usage data to link asserted identities to their pattern of usage within the eAuth system to detect potential fraudulent activities related to identity theft. Cross-channel comparison of data is necessary for a holistic analytic approach to assess the accuracy of authentication techniques and to detect potentially fraudulent account behavior after authentication. Since IRS allows business to be conducted in person at the Taxpayer Assistance Centers (TACs), via telephone with Accounts Management CSRs, and online via irs.gov, it is necessary to consult the authentication attempts across channels to understand fraudulent attempts at identity authentication, assess differences in accuracy of the different channel-based techniques, and to remediate harms caused.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration	Yes	
To provide Taxpayer Services	No	
To collect Demographic Data	No	
For employee purposes	No	
		If other, what is the use?
Other:	Yes	validate eAuth KBA in order to help prevent ID Theft in Tax Administration

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?

If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies		
Web Beacons		
Session Cookies		
Other:		*If other, specify:*

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

18a. If Yes, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Not Applicable

19a. If Yes, how does the system ensure "due process"?

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent	No
Website Opt In or Out option	Yes
Published System of Records Notice in the Federal Register	No
Other:	No

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Only
Managers		No Access
System Administrators		No Access
Developers		No Access
Contractors:	Yes	
Contractor Users		Read Only
Contractor System Administrators		No Access
Contractor Developers		No Access
Other:	No	

If you answered yes to contractors, please answer 22a. *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level"background investigation? Yes

23. How is access to the PII determined and by whom?

Cybersecurity determines access to eAuth account usage databases and eAuth Equifax reconciliation files (via 5081). Access to PII is determined by system owner based on personnel requirements for eAuth identity authentication initiative. Access is restricted only to IRS analysts and contractors. All reports generated from data will be at the aggregate level, absent PII. Access to the individual TIN level information from the DCI data is limited those assigned to identity authentication analytics in OCA, RICS, PGLD, and OLS. Access is controlled at two layers: CDW access granted by RAS and access to the specific folder in Thor granted by OCA.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

This PIA is restricted in its scope to the dissemination of an extract of eAuth account usage data and eAuth reconciliation report data from Equifax. The original data continues to be owned by Cybersecurity. Cybersecurity is responsible for monitoring eAuth account usage data for accuracy, timeliness, and completeness of SBU/PII data. Any corrections to the data in the extract stored on the shared folder on the CDW server will overwrite existing data.

25. 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

25a. 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).

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

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).

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

The CDW server will store the eAuth data extract. The data will be stored as a csv file within an OCA analyst's personal folder on the CDW server. It will not be loaded as a data table into the CDW database. The OCA analyst will restrict read/write privileges only to other OCA analysts and contractors who will analyze the data by only providing the extension of the hidden folder to those approved for access by the program manager. The data will be analyzed on the server itself rather than saving to a local drive.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

Not applicable

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

Each person granted access to PII data is required to sign a non-disclosure agreement and undergo a properly adjudicated background investigation at the level required for their access, and receive UNAX training that includes warnings that intentional unauthorized disclosure is subject to criminal penalties.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number	SORNS Name
Treas/IRS 24.030	IMF
Treas/IRS 24.046	BMF
Treas/IRS 34.037	Audit Trail and Security Records Systems

Comments

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No

32a. If Yes to any of the above, please describe:

NA

View other PIAs on IRS.gov