eAuthentication – Version 1.3 (eAuth) – Privacy Impact Assessment

PIA Approval Date – Jul. 26, 2011

System Overview:

eAuthentication was born out of the IRS internet strategy from Commissioner's strategic goal for improving service, expedite processes and improve efficiency by providing preferred online channels to reach out to customers. Internal Revenue Service (IRS) intends on delivering additional services via the Internet channel to the taxpayer and tax–prepares thereby increasing voluntary compliance and taxpayer satisfaction. It is crucial that these services be delivered in such a manner that security and privacy risk is effectively managed and controlled and the burden on the taxpayer is kept to a minimal. A key component of security and privacy would be the manner in which individual users identify (proof) themselves to the system and their subsequent re–authentication. Currently, IRS externally facing applications offer their own authentication solutions resulting in disparate silos of identity management. The eAuthentication system as such does not store any data collected. Data gathered from the taxpayer will be transmitted to the backend systems to validate the identity and authenticate the individuals to use IRS services via Internet. eAuthentication would be a common service that would identity proof/Authenticate in a consistent way with high–quality customer experience. This eAuthentication effort is sponsored by Modernization and Information Technology Services (MITS), Office of Cybersecurity, Architecture and Implementation.

Systems of Records Notice (SORN):

- 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 System

Data in the System

1. Generally describe the information to be used in the system in each of the following categories:

- Taxpayer: Information collected from the taxpayer consist of:
  - Taxpayer Name
  - Taxpayer Identification number (ITIN/SSN)
  - Taxpayer Date of Birth
  - Taxpayer Address of Record
  - Taxpayer Financial Account Number (Bank or Credit card)
  - Taxpayer Email Address
  - Taxpayer Phone Number
  - Taxpayer Filling Status

2. What are the sources of the information in the system?

Information is collected by the eAuthentication system from the taxpayer to identify the individuals before accessing the IRS services via Internet. This information is verified against the IRS data sources utilizing the services around Business Web Application Servers (BWAS) and Integrated Customer Communications Environment Web Applications (ICCE).

A. What IRS files and databases are used?

Information collected from the taxpayer is sent back to the backend systems using services around BWAS and ICCE systems.

B. What Federal Agencies are providing data for use in the system?
No. Federal Agencies are not providing data for use in the system.

C. What State and Local Agencies are providing data for use in the system?
No State or Local Agencies provide data for use in eAuthentication.

D. From what other third party sources will data be collected?
Data is not collected from any other third party sources.

E. What information will be collected from the taxpayer/employee?
Information collected from the taxpayer consist of,

- Taxpayer: Information collected from the taxpayer consist of,
  - Taxpayer Name
  - Taxpayer Identification number (ITIN/SSN)
  - Taxpayer Date of Birth
  - Taxpayer Address of Record
  - Taxpayer Financial Account Number (Bank or Credit card)
  - Taxpayer Email Address
  - Taxpayer Phone Number
  - Taxpayer Filling Status

3. A. How will data collected from sources other than IRS records and the taxpayers be verified for accuracy?
Not applicable. eAuthentication does not collect information from sources other than taxpayers.

B. How will data be checked for completeness?
The eAuthentication system uses secured channel for data transmission between end points with no data loss. During registration, the identity verification module shall return a “go” only in case of “complete” information is verified.

C. Is the data current? How do you know?
The data used for ID proofing is collected from the taxpayers .The eAuthentication system uses secured channel for data transmission between end points with no data loss. The Identity Verification module verifies the data from the back–end sources and the back–end IRS data is considered sacrosanct for current–ness.

4. Are the data elements described in detail and documented? If yes, what is the name of the document?
The data elements are documented as part of the BSAR.

Access to the Data

5. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?
System Administrators who have access to eAuthentication will have organization specified clearances and are only granted access when their jobs require it. Their access is immediately revoked when it is no longer required.

6. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access to the directory data within the system is restricted to the System Administrators. The criteria, procedures, controls and responsibilities regarding access are documented in the IRS access control documentation. The user's profile and roles are assigned by his/her manager, and are established when user accounts are created.

7. Will users have access to all data on the system or will the user's access be restricted? Explain.
The Administrator has a need–to–know level of access to the user directory. The System Administrator grants approval for system access. A user's access to the data terminates when the user no longer requires access to eAuthentication. The criteria, procedures, controls and responsibilities regarding access are documented in the IRS access control documentation.

8. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?
Taxpayer information collected by the eAuthentication system is passed to the backend system for verification. In addition eAuthentication follows IRS Security policy 10.8.1 and uses audit trails per IRM 10.8.3.

9. A. Do other systems share data or have access to data in this system? If yes, explain.
eAuthentication registration data stored in the secured directory will be available for applications to access to identify individual users. Secured channel will be used for data transmission between eAuthentication directory and applications with no data loss.

B. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?
The IRS is responsible for protecting the privacy rights of taxpayers regarding data contained within eAuthentication system.

10. A. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?
No other agencies share data or have access to the data contained in or transmitted by eAuthentication system.

B. How will the data be used by the agency?
No other agencies share data or have access to the data contained in or transmitted by eAuthentication system.

C. Who is responsible for assuring proper use of the data?
No other agencies share data or have access to the data contained in or transmitted by eAuthentication system.

D. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?
No other agencies share data or have access to the data contained in or transmitted by eAuthentication system.

Attributes of the Data

11. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?
Yes. The data gathered by the eAuthentication is both relevant and necessary to the purpose for which the system has been designed.

12. A. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?
The eAuthentication system does not derive or create previously unavailable data about an individual through aggregation from the information collected.

B. Will the new data be placed in the individual's record (taxpayer or employee)?
The eAuthentication system does not derive or create previously unavailable data about an individual through aggregation from the information collected.

C. Can the system make determinations about taxpayers or employees that would not be possible without the new data?
The eAuthentication system cannot make determinations about taxpayers.

D. How will the new data be verified for relevance and accuracy?
The eAuthentication system collects data from the taxpayers and sends it to the backend system for data validation.

13. A. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
Taxpayer information collected by the eAuthentication system will be passed to the backend system for verification. In addition eAuthentication follows IRS Security policy 10.8.1 and uses audit trails per IRM 10.8.3, to validate the user access to the eAuth system.

B. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
Taxpayer information collected by the eAuthentication system will be passed to the backend system for verification. In addition eAuthentication follows IRS Security policy 10.8.1 and uses audit trails per IRM 10.8.3, to validate the user access to the eAuth system.

14. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.
The registration data stored in the eAuthentication directory can only be accessed by application to identify users. In all cases, the data that the user enters on the UI screens during registration shall be captured and sent to the Identity–proofing module for verification. Upon verification the module returns a "yes" or "no" for the user profile to be created in the eAuth Directory.

15. What are the potential effects on the due process rights of taxpayers and employees of:

A. consolidation and linkage of files and systems;
Should have no effect on the eAuth system, as the application exposing the Identity verification module is actually a wrapper application around the back–end systems.

B. derivation of data;
Data is collected from the Taxpayers for Identification purpose.

C. accelerated information processing and decision making;
The accelerated information processing performed by the eAuthentication system does not affect the due process rights of the taxpayers. eAuthentication authenticates users' access to IRS application on the web and it does not perform any decision–making.

D. use of new technologies;
The eAuthentication system does not affect the due process rights of taxpayers.

16. How are the effects to be mitigated?
The eAuthentication system does not affect the due process rights of taxpayers.

Maintenance of Administrative Controls

17. A. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.
The eAuthentication solution is a common service that would identity proof/Authenticate taxpayers in a consistent way with high–quality customer experience. There is no possibility of disparate treatment of individuals or groups. All taxpayers are treated equally.

B. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?
The data is on a real–time replication mode across multiple geographically distributed nodes.

C. Explain any possibility of disparate treatment of individuals or groups.
The eAuthentication solution is a common service that would identity proof/Authenticate taxpayers in a consistent way with high–quality customer experience. There is no possibility of disparate treatment of individuals or groups. All taxpayers are treated equally.

18. A. What are the retention periods of data in this system?
A request for records disposition authority for eAuth and associated records is currently being drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. A 7–years and 6 months disposition is being proposed for registration records in accordance with NIST 800–63 regulations. When approved by NARA, eAuth disposition instructions will be published in IRM 1.15, exact records control schedule and item number to be determined.

B. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?
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 IRS Records Management Requirements in IRMs 1.15.3 Disposing of Records and 1.15.6 Managing Electronic Records, and records disposition instructions (to be) approved by NARA.

C. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?
The eAuthentication system uses secured channel for data transmission between end points with no data loss. During registration, the identity verification module shall return a “go” only in case of “complete” information is verified.

19. A. Is the system using technologies in ways that the IRS has not previously employed (e.g., Caller–ID)?
The eAuthentication system is not using technologies in ways that the IRS has not previously employed.

B. How does the use of this technology affect taxpayer/employee privacy?
The eAuthentication system collects taxpayer information for the purpose of Identification and Authentication.

20. A. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

No. Information retrieved from eAuthentication can contain individual taxpayer information such as name, address, and taxpayer identification number. The taxpayer information collected by the eAuthentication system will only be used for the ID proofing process and it is not being used to locate or monitor individuals.

B. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.

The taxpayer information collected by the eAuthentication system will only be used for the ID proofing process and it is not being used to locate or monitor individuals.

C. What controls will be used to prevent unauthorized monitoring?

Only authorized employees will have access to the information on eAuthentication. All employees and contractors receive UNAX and Code of Conduct training. Identification and access provisions are employed.

View other PIAs on IRS.gov