

## **e-Services, Release 3.0, Version 1.0 – Privacy Impact Assessment**

**PIA Approval Date – Dec. 17, 2007**

### **System Overview**

The E-Services (E-Services) project is a Business Systems Modernization Office project focused on revolutionizing the way taxpayers transact and communicate with the IRS. This Web-based project will expand the existing third-party tools and data collection processes.

### **Description of System**

e-Services is a suite of Web-based products that allow tax payers, tax professionals, financial institutions, and state tax representatives to conduct business with the IRS. These services are available 24 hours a day, 7 days a week, via the Internet at [www.irs.gov/](http://www.irs.gov/).

#### **e-Services is comprised of the following Sub-applications:**

##### **Business Unit:**

W&I

##### **Sub-application Name:**

Registration

##### **Sub-application Function:**

Allows a third party to register online to use e-Services products; individuals must register to create and have access to a secure mailbox. The registration process is a one-time automated process where the user selects a username, password and PIN that is needed to log onto e-Services. A paper based Registration option is available but only for residents of Puerto Rico and victims of identity theft.

##### **Business Unit:**

SB/SE

##### **Sub-application Name:**

Preparer Taxpayer Identification Number (PTIN) Application

##### **Sub-application Function:**

Allows a third party to apply on-line for a PTIN and provides the option to request input a paper application.

##### **Business Unit:**

W&I

##### **Sub-application Name:**

e-File Application

##### **Sub-application Function:**

Allows a third party to apply on-line to become an e-Filer and provides the option to request input a paper application.

##### **Business Unit:**

SB/SE

##### **Sub-application Name:**

Interactive and Bulk TIN Matching

##### **Sub-application Function:**

Allows a third party to check the correlation of Taxpayer Identification Number (TIN) with names prior to filing an information return to the IRS. Interactive TIN matching allows a third party to match up to 25 TIN and name combinations during an on-line session. Bulk TIN matching allows a third party to match up to 100,000 TIN and name combinations and receive results within 24 hours.

**Business Unit:**

W&amp;I

**Sub-application Name:**

Transcript Delivery System (TDS)

**Sub-application Function:**

Allows authorized tax professionals and IRS employees to submit a request for transcripts (return transcripts, account transcripts, record of account, wage and income documents, and verification of non-filing products) electronically and receive them on-line or via their secure mailbox.

**Business Unit:**

W&amp;I

**Sub-application Name:**

Disclosure Authorization (DA)

**Sub-application Function:**

Allows an authorized tax professional to submit a Power of Attorney or Tax Information Authorization electronically.

**Business Unit:**

W&amp;I

**Sub-application Name:**

Electronic Account Resolution (EAR)

**Sub-application Function:**

Allows an authorized tax professional to expedite closure on clients' account problems by electronically sending/receiving account related inquiries.

**Business Unit:**

W&amp;I

**Sub-application Name:**

Indirect Channel Management (ICM)

**Sub-application Function:**

Allows an IRS user to recruit and manage partner relationships.

**Data in the System****1. General Description of Data by Category****1.a. Generally describe the taxpayer information to be used in the system**

Users in the role of registrant or applicant (tax practitioner, Electronic Return Originator (ERO), state tax representative, payer, etc of the e-Services system are required to provide personal taxpayer information which consists of:

- name
- address
- date of birth
- SSN – used for the Registration process and is one of the shared secrets that are used to ensure the person is who they say they are.
- user identification (User ID)
- password and personal identification number (PIN)
- correspondence information (e-mail, telephone, & fax)
- adjusted gross income (AGI)
- AGI Year

- Individual Taxpayer Identification Number (ITIN)
- Preparer Taxpayer Identification Number (PTIN)

### **1.b. Generally describe the employee information to be used in the system**

- IRS employee names
- Standard Employee Identifier (SEID)
- email
- Telephone number (work)
- Work address
- password

### **1.c. Generally describe any other Personally Identifiable Information (PII) to be used in the system**

- role within the Business (of the business name listed)
- professional status information
- fingerprint cards (to determine suitability)- (name of individual, if a fingerprint card exists, and the date that the fingerprint card came back from FBI)
- Flag indicating whether or not the individual has a criminal background (as determined by the FBI)
- Employer Identification Number (EIN)
- Responses to question on past criminal record (whether an individual committed a criminal act, if so, what was the citation, etc...?)
- Results of Suitability Checks, is the individual and business compliance with their taxes and or been assessed penalties.

## **2. Sources of Information in the System**

### **2.a. What IRS files and databases are used?**

- Enterprise Directory and Authentication Service (EDAS)
  - Authentication data (user ID and Password)
  - PIN
  - User roles
- Third Party Data Store—Provides third party registrant information for use with e-Services Products
- Transitional Database (XDB)- supports e-Services with validation. Provides e-Services with:
  - National Account Profile
  - National Account Profile Social Security (SS) File
  - National Account Profile Social Security Number
  - Spouse's Cross Reference
  - Payer Authorization File
  - Return Transaction Information (Adjusted Gross Income (AGI) and AGI Year)
  - Employer Identification Number and Name Controls
  - Name Control data (part of National Account Profile)
  - Enrolled Agent Information (status of the individual for purposes of validating the data that is entered to e-file)

The e-Services Products will use business and individual taxpayer related information. UWRs have been submitted for each system as required. The following list identifies the data that is needed and interface purpose for the current files:

- Standard Corporate Files On Line (CFOL) Access Protocol (SCAP)—Contains:
  - Individual Return Tax File On Line (IRTFOL)
  - Business Return Tax File On Line (BRTFOL)
  - Information Return Master File On Line (IRMFOL)
  - Individual Master File On Line (IMFOL)
  - Business Master File On Line (BMFOL)
  - Individual Return Transaction File (IRTF)
  - Business Return Transaction File (BRTF)
  - Individual Return Master File (IRMF)
  - Business Master File (BMF) Retention Register Files
  - Individual Master File (IMF) Retention Register Files
- Centralized Authorization File (CAF)—Establishes taxpayer and Third Party relationships for disclosure authorization. (This information is not imported to e-Services, but rather used to validate in real-time against it)
- Desktop Integration (DI)
- Electronic Filing System /Individual Master File (IMF BMF)
- Employer Identification Number Name Control File (EIN/NC)
- Enrolled Agent (EA)
- ETA Research and Analysis System (ETARAS)
- Modernized E-file- MEF- provides tax return information
- National Account Profile SS File (NAP-SS)
- National Account Profile SSN File (NAP-SSN)
- Payer Authorization File (PAF)—Subset of the Payer Master File (PMF) that holds information (valid Payer ID Number and EIN) about the individual or entity that actually pays the taxpayer obligation.
- Preparer Tax Identification Number (PTIN)(this is an IRS file)
- Reporting Agent File (RAF) – Establishes business taxpayer and third party relationships for disclosure authorization. (This information is not imported to e-Services, but rather used to validate in real-time against it)
- Return Transaction File (RTF)
- Spouse's Cross Reference File (XREF)
- Telephone Routing Interactive System / Interactive Processor (TRIS/IP)
- Transaction Code 120 (TC120) Transactions to Disclosure File – TC120 record of disclosure when a taxpayer's transcripts are disclosed to a state tax representative
- Unified Location Code (ULC)/Zip- valid zip code file

## **2.b. What Federal Agencies are providing data for use in the system?**

e-Services receives information from the Federal Bureau of Investigation (FBI) as part of the suitability background checks on some applicants who do not have professional credentials. This information is received through the Automated Electronic Fingerprint (AEF) system. The IRS receives Social Security Number, date of birth and other data elements (e.g. Date of death) from the Social Security Administration.

## **2.c. What State and Local Agencies are providing data for use in the system?**

e-Services receive no information from state and local agencies.

## **2.d. From what other third party sources will data be collected?**

Pending Disclosure Authorization- data that is collected from the external user. The file temporarily stores pending DA transactions awaiting third party and taxpayer signatures up to 7 days. Information is collected from Taxpayers and representatives (the individuals whom the taxpayer is authorizing to receive their refund or who are being allowed to represent them.)

Transaction History Database—provides application specific transaction elements for use by IRS management and the e-Services such as; TIN matching, DA, TDS, and EAR applications.

Log File Collector – stores transaction audit record information

## **2.e. What information will be collected from the taxpayer/employee?**

### **Taxpayer:**

- AGI
- AGI Year
- self selected PIN
- Address
- TIN and daytime telephone number
- Date Of Birth (DOB)
- Email address
- Tax period
- Tax form
- Fax number
- Negative Taxpayer Identification Number (TIN) (represents the TINS of the transcripts which the employee is prevented from viewing (such as family members, themselves, etc.)

**Employee:** No information is collected directly from the employee.

## **3. Verification of Accuracy, Completeness, and Timeliness**

### **3.a. How will the data collected from sources other than IRS records and the taxpayers be verified for accuracy?**

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.

### **3.b. How will data be checked for completeness?**

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.

### **3.c. Is the data current? How do you know?**

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. When a user accesses registration data, it accesses the Transactional DataBase (XDB) for that information. The taxpayer address is updated on a recurring basis. If a taxpayer updates an address it will post within the masterfile. e-Services will receive the updated address within one week.

## **4. Description of Data Elements**

### **4.a. Are the data elements described in detail and documented?**

Yes.

### **4.b. If the answer to question 4.a. is yes, what is the name of the document?**

A Data Model View document is maintained as part of system documentation which is regularly updated. The document details the e-Services data elements and their location within the system.

## **Access to the Data**

### **1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?**

There are two types of users supported by e-Services: internal and external. The IRS is considered an internal user. Non-IRS is considered external users. Third-party users (external) are qualified as either registrants or applicants

#### **Internal users are categorized into the following roles:**

**Role:** Developers

**Permissions:** Access to live data, only able to read. Cannot delete.

**Role:** System Administrator

**Permissions:** Do not have access to live data. System administration privileges.

**Role:** Users

**Permissions:** Access to live data, cannot delete, able to read and write data through normal course of using applications.

Contractors hold roles as internal users. To operate as an internal user a contractor is required to hold a Live Data Waiver which is authorized through their manager or COTR.

Contractors are also required to have a clearance level which permits Staff-like Access.

#### **External users are categorized into the following roles:**

**Role:** Registrant

**Permissions:** A registrant is an individual taxpayer who is seeking access to IRS electronic services and is allowed access to the Registration Web page. A registrant is granted rights to only his or her unique registration data. A registrant may view and modify specific data fields, such as address, phone number, password, and PIN. Registration is the basic level privilege granted to third-party users and must be completed before additional electronic service privileges are granted. This is the necessary first step for third-party users to identify themselves and the IRS to authenticate their identity.

**Role:** Applicant

**Permissions:** An applicant is a legal entity that may act on the behalf of an individual taxpayer or other authorizing organization

## 2. User Access Determination Procedures

### 2.a. How is access to the data by a user determined?

IRS employees request access to specific applications on the Employee User Portal (EUP) by submitting an Online 5081. Managerial approval is required.

Registrants are allowed access to electronic services after they complete an on-line application or paper-based registration process and have been assigned privileges by the applicant's Principal, Principal Consent, or Responsible Official.

In practice, 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.

### 2.b. Are criteria, procedures, controls, and responsibilities regarding access documented?

Criteria, procedures, controls, and responsibilities regarding access are those that apply to OL5081.

## 3. User Access Limitations

### 3.a. Will users have access to all data on the system or will the user's access be restricted? Explain.

User access will be restricted and limited within and across the sub-applications using role-based privileges. The details of each user role and corresponding permissions can be found in the PIA documentation for each application.

### 3.b. What controls are in place to prevent the misuse (e.g. browsing) of data by those having access?

For internal users, there are UNAX and Negative-TIN controls which are in place to note the limitations of each user's access.

For external users, each user is only able to access the transcript for which they are authorized to receive by the Taxpayer.

## 4. Data Sharing within the IRS

### 4.a. Do other systems share data or have access to data in this system? If yes, explain.

e-Services interfaces with many IRS applications/systems to send and/or receive e-Services data. A description of each interface is provided below:

**Automated Suitability Analysis Program (ASAP)**- daily export from e-Services containing Taxpayer and Business data that is run against Master File to determine the Individual and Business are in compliance with their Tax obligations.

**Distribution Channel Management (DCM)** – e-Services sends all data about e-File: company name, address, telephone number, principal, responsible official, contacts (name and

telephone number), EFIN, ETIN, status of EFIN and ETIN (i.e. dropped, inactive, active), provider option (i.e. ERO, transmitter), and provider status to DCM via FTP.

**Desktop Integration (DI)**- e-Services send EAR information to PPS via DI so the account inquiry can be resolved. DI sends the PPS Assistors response back to e-Services for posting to the requesters SOR.

**e-Help Desk Support System** – A support network that provides technical assistance to external users of electronic products, and services. e-Services sends customer contact data (name, phone, address, etc.) that is being added or changed to a user's e-File application (in Extensible Markup Language [XML] format) from the e-Services Third-Party Data Store (TPDS) to the e-Help desk via information broker messages.

**Electronic Filing of 94X XML Returns (94X-XML)** – 94X-XML receives Electronic Filer Identification Number (EFIN), company name, contact name, contact telephone number, forms, and form status, software IDs via FTP from e-Services. Daily Extract

**Electronic Fraud Detection System (EFDS)**- weekly export from e-Services containing ERO data from the e-file application sub application.

**Electronic Management System (EMS)** – EMS receives software developer and Transmitters passwords, Login IDs, form information and Company name via FTP from e-Services.

**Enterprise Directory and Authentication Service (EDAS)**- provides user roles and authentication data

**ERO Locator File** – e-Services sends Electronic Return Originator (ERO) information (company name, address, and telephone number) via FTP to the ERO Locator File on a Server in Andover.

**ETA Research and Analysis System (ETARAS)** – e-Services receives EFIN number; number of transmitted, accepted, and rejected returns via FTP from ETARAS. E-Services sends ETARS a history file, a masterfile and partner file monthly via FTP.

**Exam Preparer Database** – e-Services sends all PTIN information via FTP to the Exam Preparer Database.

**Freedom of Information Act (FOIA) Extracts** – e-Services makes data available to the public (on the IRS Website) through FOIA extracts on information retrieved from the Third Party Data Store (TPDS). Available via CD upon demand.

**Integrated Data Retrieval System (IDRS)** – The IDRS application consists of the Centralized Authorization File (CAF) and the Reporting Agent File (RAF). e-Services sends the CAF number, taxpayer information, tax year, tax form, and representative information to CAF through TTB via AMDAS. e-Services receives a result code from CAF to validate the information that was sent. e-Services sends the RAF number, EIN, tax year and tax form to RAF through TTB via AMDAS. e-Services receives a result code from RAF to validate the information that was sent.

**Integrated Financial System (IFS)** – e-Services sends billing information to include company name, address, consolidator locator number, and billing data to IFS via FTP.



**Marketing Research Database (MRD)**- e-Services data is quarterly exported via FTP and contains e-filer information from the e-file applications.

**Modernized e-File (MeF)** – e-Services sends EFIN, ETIN, and contact information files via FTP to the MeF application. MeF A2A verifies and extracts the ETIN number from e-Services based on the Customer ID in an interactive on-demand access. e-Services receives information regarding electronic e-filing statistics from MEF.

**National Print System (NPS)** – e-Services sends formatted files to NPS via FTP to generate PTIN letters, TDS transcripts, and Registration letters for printing and mailing to the user.

**Transitional Database**- Provides data to support validation procedures.

e-Services relies on multiple MITS General Support Systems (GSS) located throughout the IRS Wide Area Network (WAN). The MITS infrastructures used by e-Services provide multiple layers of support and security for the application, including, but not limited to, boundary security, physical security, maintenance support, network connectivity, and alternate processing. A description of each interconnected GSS is provided below:

- MITS-1 IRS Perimeter Security.
- MITS-15 Contact Center
- MITS-17 Enterprise Systems Domain.
- MITS-18 Infrastructure Shared Services (ISS)
- MITS-20 IBM ICS/ACS/PRINT (IAP) Platform.
- MITS-22 IBM Security and Communication Platform.
- MITS-26 Enterprise Remote Access (ERAP)
- MITS-27 Modernization Test and Development Environment Domain
- MITS-30 Wintel Application Servers
- MITS-32 IRS Workstations and Support
- MITS-34 Enterprise Network.

**4.b. Who will be responsible for protecting the privacy rights of the taxpayers and employees affected by the interface?**

The Business System Owner is responsible for protecting the privacy rights of the taxpayers and employees affected by the interface.

**5. Data Sharing With Other Agencies**

**5.a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, & Other)?**

Yes, offices of the Department of Defense and the Department of Justice have access to the e-Services application.

e-Services is accessible by tax payers, tax professionals, financial institutions, and state tax representatives to conduct business with the IRS.

Since there are no interconnections between e-Services and systems external to the IRS, no MOU/ISA is required; however e-Services maintains Memorandums of Agreement (MOA) between the IRS and each state department, and Interface Control Documents (ICD) for the interfaces between e-Services and other IRS systems/components. A Memorandum of Agreement (MOA) is in place with all state users.

**Memorandums of Agreement.** The MOAs referenced below are stored in hard copy at the New Carrollton Federal Building by the W&I Business System Security Office (BSSO).

- *Memorandum of Agreement (MOA) between IRS and the Alabama Department of Revenue (11/13/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Arkansas Department of Finance and Administration (11/13/2006)*
- *Memorandum of Agreement (MOA) between IRS and Arizona Department of Revenue (11/2/2006)*
- *Memorandum of Agreement (MOA) between IRS and California Franchise Tax Board (3/1/2007)*
- *Memorandum of Agreement (MOA) between IRS and the District of Columbia Office of the Chief Financial Officer (12/21/06)*
- *Memorandum of Agreement (MOA) between IRS and the Colorado Department of Revenue (2/12/2007)*
- *Memorandum of Agreement (MOA) between IRS and the Connecticut Department of Revenue Services (1/19/2007)*
- *Memorandum of Agreement (MOA) between IRS and the Delaware Division of Revenue (1/19/2007)*
- *Memorandum of Agreement (MOA) between IRS and the State of Hawaii Department of Taxation (12/13/06)*
- *Memorandum of Agreement (MOA) between IRS and the Idaho State Tax Commission (11/2/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Illinois Department of Revenue (12/6/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Indiana Department of Revenue (12/6/2006)*
- *Memorandum of Agreement (MOA) between IRS and Iowa Department of Revenue (11/13/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Kansas Department of Revenue (11/2/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Kentucky Department of Revenue (12/6/2006)*
- *Memorandum of Agreement (MOA) between IRS and Maine Revenue Services (11/24/2006)*
- *Memorandum of Agreement (MOA) between IRS and Massachusetts Department of Revenue (11/13/2006)*
- *Memorandum of Agreement (MOA) between IRS and Comptroller of Maryland (11/20/2006)*
- *Memorandum of Agreement (MOA) between IRS and Michigan Department of Treasury (12/21/06)*
- *Memorandum of Agreement (MOA) between IRS and the Minnesota Department of Revenue (12/6/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Mississippi State Tax Commission (11/20/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Missouri Department of Revenue (11/20/2006)*
- *Memorandum of Agreement (MOA) between IRS and Nebraska Department of Revenue (11/2/2006)*

- *Memorandum of Agreement (MOA) between IRS and New Mexico Taxation & Revenue Department (12/13/2006)*
- *Memorandum of Agreement (MOA) between IRS and New Jersey Division of Revenue (11/24/2006)*
- *Memorandum of Agreement (MOA) between IRS and the New York State Department of Taxation and Finance (11/24/2006)*
- *Memorandum of Agreement (MOA) between IRS and North Carolina Department of Revenue (12/6/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Office of State Tax Administrator, State of North Dakota (11/2/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Ohio Department of Taxation (11/2/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Oklahoma Tax Commission (11/20/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Oregon Department of Revenue (11/20/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Pennsylvania Department of Revenue (1/19/2007)*
- *Memorandum of Agreement (MOA) between IRS and Rhode Island Division of Taxation (12/6/2006)*
- *Memorandum of Agreement (MOA) between IRS and South Carolina Department of Revenue (12/13/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Utah State Tax Commission (11/13/2006)*
- *Memorandum of Agreement (MOA) between IRS and the Virginia Department of Taxation (11/20/2006)*
- *Memorandum of Agreement (MOA) between IRS and the West Virginia State Tax Department (12/21/2006)*
- *Memorandum of Agreement (MOA) between IRS Wisconsin Department of Revenue (11/24/2006)*

**5.b. How will the data be used by the agency?**

External IRS sources utilize e-services to facilitate business (state tax administration/state e-file) with the IRS via obtaining e-File application information. All external IRS activity is done under a standing MOA.

**5.c. Who is responsible for assuring proper use of the data?**

Stated within each Memorandum of Agreement is the detailed responsibility of a Federal-State Liaison responsible for assuring proper use of the data.

**5.d. How will the system ensure that agencies only get the information they are entitled to under IRC 6103?**

State users have a role that specifically enables them to have access to files with preapproved fields. The data elements contained in the file have been approved by the Office of Disclosure for the purpose of sharing with the states for tax administration.

**Attributes of the Data**

**1. Is the use of the data both relevant and necessary to the purpose for which the system was designed?**

Yes, the data is needed to deliver the products.

## 2. Derivation of new data

### 2.a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

**Taxpayer:** Yes. e-Services, through aggregation, creates new data which notes whether or not the individual is allowed or not allowed to participate in e-file. Tax information on MasterFile and personal information submitted by taxpayers aggregated to create a status (Rejection versus acceptance to complete e-File application)

**Employee:** No.

### 2.b. Will the new data be placed in the individual's record (taxpayer or employee)?

**Taxpayer:** The suitability determination does not go into taxpayer record. The determination is placed in the individuals' profile, not tax record and is not considered taxpayer information.

**Employee:** No.

### 2.c. Can the system make determinations about taxpayers or employees that would not be possible without the new data?

**Taxpayer:** Yes, when an individual is noted as rejected for e-File participation, e-Services prevents them from submitting other e-file applications. Yes, it has made a determination on the taxpayer's profile. This determination completed as stated above (2a).

**Employee:** No, all participants will be treated equally based on their roles. Users will receive access to E-services Products based on the roles approved by their Manager.

### 2.d. How will the data be verified for relevance and accuracy?

The individual is provided written notification of their status (rejection or acceptance) and provided appeal rights to question the determination and accuracy.

## 3. Consolidation of Data and Processes

### 3.a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.

Usernames and passwords, and in certain instances also PINS, are required by users to establish and/or access data in the systems.

### 3.b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Yes, all e-Services applications require authorized role-based access controls and validate preapproved authorizations to enable transactions to occur.

## 4. Data Retrieval

### 4.a. Can the data in the system be retrieved by personal identifier?

Yes. User ID, password, and PIN can be used to retrieve data.

### 4.b. If the answer to question 4.a. is Yes, how will the data be retrieved?

using certain fields (below) to retrieve records

- address
- TIN
- Preparer Tax Identification Number (PTIN) - this retrieves the PTIN application itself.
- user identification (Login ID)

- EFIN
- ETIN
- Telephone number
- Company name
- Username
- SEID (allows access to registration data)
- Consolidator Number

## 5. Due Process Rights

### 5.a. What are the potential effects on the due process rights of taxpayers and employees as a result of consolidation and linkage of files and systems?

**Taxpayer:** the taxpayers are provided appeal rights when the consolidation of data results in an adverse effect.

**Employee:** Not Applicable.

### 5.b. What are the potential effects on the due process rights of taxpayers and employees as a result of derivation of new data?

**Taxpayer:** the taxpayers are provided appeal rights when the consolidation of data results in an adverse effect

**Employee:** Not Applicable.

### 5.c. What are the potential effects on the due process rights of taxpayers and employees as a result of accelerated information processing and decision making?

**Taxpayer:** N/A. Any acceleration has not changed a taxpayer's ability and time to appeal. The taxpayers are provided appeal rights when the consolidation of data results in an adverse effect

**Employee:** Not Applicable.

### 5.d. What are the potential effects on the due process rights of taxpayers and employees as a result of the use of new technologies?

**Taxpayer:** The use of new technologies by e-Services will enable better protection against unauthorized access and does not affect due process rights.

**Employee:** The use of new technologies by e-Services will enable better protection against unauthorized access and does not affect due process rights.

### 5.e. How are the effects on due process rights to be mitigated?

No effects on due process rights have been identified. No mitigation is necessary.

## Maintenance of Administrative Controls

### 1. Equitable and Consistent Treatment of Taxpayers and Employees

#### 1.a. Explain how the system and its use will ensure equitable treatment of taxpayers and employees.

e-Services provides consistent application of business rules for equitable treatment for all users. Users will receive access to e-Services based on the roles assigned by their Principal, Principal Consent, and/or Responsible Official.

#### 1.b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?

Established roles and access permissions are location-wide.

**1.c. Explain any possibility of disparate treatment of individuals or groups.**

As per the consistent application of business rules that is implemented there are no possibilities for disparate treatment.

**2. Data Retention and Elimination**

**2.a. What are the retention periods of data in this system?**

e-Services component applications each maintain their own procedures for retention and retention periods, as determined by each component Business Owner (and detailed in their respective PIAs). e-Services components retention periods range from one month to three years.

**2.b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?**

The records will be maintained in accordance with Records Disposition Handbooks, IRM 1.15.59.1 through IRM 1.15.59.32. All data meeting end of retention period requirements will be eliminated, overwritten, degaussed, and/or destroyed in the most appropriate method based upon the type of storage media used.

CR-145 - e-Services transmits extracted files to other IRS systems. The extracted files are written to a temporary storage area and are deleted after the transmission. The file deletion process was tested and confirmed during e-Services 1.2 release ST&E testing. After transmitting the data procedures listed in Records Disposition Handbooks, IRM 1.15.59.1 through IRM 1.15.59.32 are followed. All data meeting end of retention period requirements will be eliminated, overwritten, degaussed, and/or destroyed in the most appropriate method based upon the type of storage media used.

**2.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?**

All determinations are made utilizing e-Services data which is updated on a reoccurring and regular basis.

**3. Use of New Technology**

**3.a. Is the system using technologies in ways that the IRS has not previously employed (e.g. Caller-ID)?**

No.

**3.b. How does the use of this technology affect taxpayer/employee privacy?**

As technology will not be used in ways that the IRS has not previously employed, there will be no effect on taxpayer/employee privacy.

**4. Location and Monitoring of Individuals and Groups**

**4.a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

As per the consistent application of business rules that is implemented there are no possibilities for monitoring individuals.

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

As per the consistent application of business rules that is implemented there are no possibilities for monitoring groups.

**4.c. What controls will be used to prevent unauthorized monitoring?**

Access controls based on user profile information prevent this activity.

Management's commitment to employee UNAX training keeps them aware of the need to be good stewards of the public trust.

**5. System of Records Notice (SORN) Specifications**

**5.a. Under which SORN does the system operate? Provide number and name.**

- Treasury/IRS 24.030—Individual Master File (IMF), Taxpayer Services (formerly Individual Master File (IMF), Returns Processing)
- Treasury/IRS 24.046—Business Master File (BMF), Taxpayer Services (formerly Business Master File (BMF), Returns Processing)

**5.b. If the system is being modified, will the SORN require amendment or revision?**

**Explain**

No.

[View other PIAs on IRS.gov](#)