

My IRS Account (MIRSA) Release 1, Milestone 4b - Privacy Impact Assessment

PIA Approval Date - July 25, 2008

Requested Operational Date - August 25, 2008

System Overview:

The My IRS Account (MIRSA) application offers online tax account services to 1040-series taxpayers through a self-service Internet application. MIRSA is aimed at the individual taxpayer, and does not provide an interface for businesses or third parties. Through the MIRSA application, individual taxpayers can securely view account information without IRS Customer Service Representative (CSR) assistance.

Systems of Records Notice (SORN):

- 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 Records System

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer:

Taxpayer information gathered from users at log-in by the ITAS subsystem of MIRSA includes:

- First Name
- Last Name
- Social Security Number (SSN)/Individual Taxpayer Identification Number (ITIN)
- Date of Birth (DOB)
- Street Address
- Personal Identification Number (PIN)
- Caller ID
- Balance Due
- Expected Refund Amount
- Total Credit
- Total Payment
- Total Tax
- Adjusted Gross Income (AGI)
- ITAS Username
- ITAS Password

With the exception of ITAS username and password, all of the above-mentioned data elements are validated against IRS legacy (non-modernized) data systems/data sources, including the Integrated Data Retrieval System (IDRS) and Corporate Files Online (CFOL). The ITAS username and password data elements are validated against the ITAS authentication database.

Taxpayer information retrieved from back end components and maintained as part of an MIRSA application session includes:

- Tax Year(s)

- Summary of Account
 - Primary Name
 - Primary SSN
 - Primary TIN Type
 - Filing Status
 - Date of Birth
 - Address Type
 - Caller ID (from notice)
 - Dwelling Number
 - Street
 - City
 - Zip
 - In Care of Name
 - Exemptions
 - AGI
 - Taxable Income
 - Tax per Return
 - Tax Period
 - Tax Return Type
 - SE Taxable Income – Taxpayer
 - SE Taxable Income – Spouse
 - Total Self Employment Tax
 - Return Due Date or Return Receive Date (whichever is later)
 - Processing Date
 - Account Balance
 - Accrued Interest
 - Accrued Penalty
 - Account Balance plus Accruals
 - Assessed Late Payment
 - Interest Paid
 - Payoff Amount
 - Payoff Computation Date
 - Installment Payment Amount
 - Installment Payment Day
- Transactions
 - Date
 - Explanation of Transaction
 - Amount
- Tax years for which tax return information is available
- Tax years for which a photocopy is available
- Pending Payments
 - Date Received
 - Amount
 - Tax Year
 - Notes
- Tax return summary
 - Name(s) shown on the return
 - SSN
 - Spouse SSN
 - Form Number

- Tax Period
- Tax Return Type
- Filing Status
- Exemptions
- AGI
- Taxable Income
- Tax per Return
- Dependant Information
- Received Date
- Preparer ID
- Expected Refund Amount
- Dependant 1 Name/SSN
- Dependant 2 Name/SSN
- Tax return information for the year specified
 - Description
 - Amount

It should be noted that all taxpayer data that is accessed by MIRSA is stored in IRS legacy data systems/data sources, including IDRS and CFOL. No taxpayer data is permanently stored or maintained by the MIRSA application.

B. Employee:

No IRS employee data is available in the MIRSA application because IRS employees do not use the MIRSA application to view taxpayer data. There are no internal components of MIRSA that are accessible to IRS employees (i.e., an MIRSA administrative component). IRS employees have the ability to utilize the MIRSA application as taxpayers, meaning they are required to authenticate in the same manner as taxpayers and can only view their own IRS account data.

C. Audit Trail Information:

MIRSA audit data is captured by the Security Audit and Analysis System (SAAS). Audit trail logging for the application is sent to SAAS via Application Messaging and Data Access Services (AMDAS). Audit records contain the following data:

- ITAS Username
- Event Type (i.e., view tax return details – refer to the MIRSA System Security Plan (SSP) for a comprehensive listing of auditable events)
- Taxpayer Identification Number (TIN)
- IP Address
- Session ID
- Success/failure of event
- Event-specific data (i.e., SSN, TIN type, file source, ITAS username)
- Timestamp

Additionally, MIRSA collects Management Information System (MIS) data related to the taxpayer's use of the application (e.g., how many hits encountered, how many times the "View Account Summary" service is accessed). These reports contain high-level summary statistics and do not contain any personally identifiable information (PII).

D. Other:

N/A. No other data is available in the application.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS:

MIRSA retrieves IRS data from the IDRS and CFOL systems using the Account Information Summary Download (AISDL), Legacy Index (LINDX), and Standard CFOL Access Protocol (SCAPD) command codes.

Refer to question 1A of this PIA for specific information about the data elements that are obtained from IDRS and CFOL.

B. Taxpayer:

The PII that taxpayers submit online in order to gain access to their individual IRS account information is referenced in question 1A of this PIA.

C. Employees:

Employees do not provide information to the MIRSA application. As such, the MIRSA application does not obtain any data from employees.

D. Other Federal Agencies:

No other federal agencies provide data to MIRSA.

E. State and Local Agencies:

No state and local agencies provide data to MIRSA.

F. Other third party sources:

No other third party sources provide data to MIRSA.

3. Is each data item required for the business purpose of the system? Explain.

Yes. The business purpose of MIRSA is to allow authenticated taxpayers to view their IRS account information through the Internet without IRS Customer Service Representative (CSR) assistance, so individual taxpayer account data stored in IDRS and CFOL is required to achieve the business purpose of the system. Each data item is used either to verify authenticity of the taxpayer or to provide the information the taxpayer is requesting.

4. How will each data item be verified for accuracy, timeliness, and completeness?

Tier 1 and Tier 2 authentication data provided by taxpayers is validated against IRS records in IDRS and CFOL. After these pieces of data are validated successfully, a user must create a username and password in order to access the application. Usernames and passwords are validated against the ITAS authentication database.

MIRSA verifies user input through the use of multiple mechanisms. At the front end, the MIRSA application restricts user input through the use of JavaScript that notifies the user if sections of the form were left blank or the input was a different type than what is acceptable for the field. It should be noted that the application functions in the same manner regardless of whether JavaScript is disabled. If JavaScript is disabled, instead of displaying pop-up messages, the user is taken to a re-enter page where they are asked to verify their input. The application also notifies the taxpayer through the use of "on screen" text examples of input restrictions.

At the business tier, business rules exist to specify the allowable lengths, formats, and data types for each application input field. Additionally, all data entered on the MIRSA application user interfaces is checked at the presentation and business tiers to ensure that null values or values exceeding the allowed field widths are prevented from creating system errors. Furthermore, when MIRSA retrieves data from IRS legacy systems/data sources, MIRSA compares the TIN sent in the request to the TIN sent in the response to ensure that the correct record has been returned.

5. Is there another source for the data? Explain how that source is or is not used.

No. MIRSA receives authentication data from taxpayers and retrieves data to be displayed to taxpayers from the legacy IRS systems noted in question 2A of this PIA.

6. Generally, how will data be retrieved by the user?

Data is retrieved from IRS records by the user through the publicly available Web front end portion of the application using a standard 128-bit Secure Sockets Layer (SSL) encryption capable Web browser such as Internet Explorer or Netscape Navigator. Taxpayers have no direct access to IRS systems beyond the supporting front end Web servers on which MIRSA resides (i.e., IRS legacy systems, such as IDRS and CFOL, where taxpayer account information is stored). Taxpayers only have access to the front end components of the MIRSA Web servers as is necessary to provide MIRSA with information to perform its intended purpose and view the resulting information display. Taxpayers only have access to their own IRS account information.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?

Yes. All MIRSA users are required to create a username and password through ITAS in order to gain access to MIRSA. In order to create this username and password, users must successfully provide a combination of shared secrets in support of Tier 1 authentication, as well as amounts from tax forms on file with the IRS in support of Tier 2 authentication. Specifically, the following information is required as part of Tier 1 authentication:

- First Name
- Last Name
- SSN/ITIN
- DOB
- Street Address

After Tier 1 authentication data is validated, users are required to provide combinations of PIN, caller ID, and tax return-related amounts for Tier 2 authentication. Once this information is validated against IRS legacy systems and the user successfully creates a username and password, the user is granted access to MIRSA and is given access to their individual IRS account information.

Access to the Data

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

- Internal Users:
 - Business managers have access to MIS data.
 - Security administrators have access to audit data stored in SAAS.
 - System administrators (SAs) and database administrators (DBAs) have access to the ITAS authentication and session databases.

- Developers have access to their development machines and the application qualification testing (AQT) environment. Developers have no access to live data.
- Contractors, including developers, do not have direct access to the MIRSA production system or authentication database. Only IRS SAs and DBAs have access to the production environment. However, developers are available to help SAs troubleshoot technology problems. In these cases, the SA provides the necessary information to the developer so he/she can assist with the problem, which is considered indirect access since the SA provides the developer with the necessary information as opposed to the developer being able to access it directly.

It should be noted that there are no internal components of MIRSA that are accessible to IRS employees (i.e., an MIRSA administrative component). IRS employees have the ability to utilize the MIRSA application as taxpayers, meaning they are required to authenticate in the same manner as taxpayers and can only view their own IRS account data.

- External Users:
 - There is only one (1) user role available through the MIRSA application – the role of the taxpayer. Taxpayers only have the ability to view their own IRS account information after successful authentication through ITAS.
 - Role: External user (taxpayer)
 - Permissions: View individual IRS account data

9. How is access to the data by a user determined and by whom?

- Internal Users:
 - Only authorized IRS SAs and DBAs have access to the data stored on the ITAS authentication and session databases and the data stored in legacy IRS systems. Contractors do not have direct access to the ITAS authentication and session databases or legacy IRS systems. Access to this data is determined by business need and is requested via the IRS Online 5081 (OL5081) system. SAs and DBAs first receive approval to access the data by their manager and then their OL5081 request is approved by the business owner or designee per IRS policy.
- External Users:
 - A taxpayer gains access rights to MIRSA after completing authentication through ITAS. Taxpayers are required to enter combinations of shared secrets in order to identify themselves as part of Tier 1 and Tier 2 authentication, and are then required to create a unique username and password to gain access to MIRSA. Access enables taxpayers to view their individual IRS account data. For additional information about the data elements required for taxpayer authentication, refer to question 7 of this PIA.

10. Do other IRS systems provide, receive, or share data in the system?

Yes.

MIRSA retrieves IRS data from the IDRS and CFOL systems using the AISDL, LINDX, and SCAPD command codes. For information about the data that is retrieved by MIRSA from these systems, refer to question 1A of this PIA. After successful authentication, taxpayers have the ability

to access their individual IRS account data. All taxpayer data is stored in IDRS and CFOL and is accessed by the MIRSA application during a user's session.

MIRSA sends audit data to SAAS via AMDAS. For a listing of the data elements that are sent to SAAS, refer to question 1C of this PIA.

MIRSA sends authentication credentials to the Internet Refund Fact of Filing (IRFOF) and Online Payment Agreement (OPA) applications for authenticated MIRSA users who click links to these pre-existing Web applications so that these users do not have to re-authenticate to IRFOF and OPA in order to gain access to the functionality provided by these applications. These authentication credentials are sent via a session cookie that is destroyed at the end of a user's session and consist of shared secrets, such as name, SSN, DOB, and expected refund amount.

MIRSA sends transcript requests to the eServices Transcript Delivery System (TDS). Specifically, MIRSA sends a TIN, tax period, master file transaction code (MFT), and other supporting information to TDS. TDS then prepares and sends the requested transcript for printing and mailing. MIRSA sends data to TDS via the File Transfer Protocol (FTP).

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?

Yes.

IDRS:

- C&A approved on May 18, 2006, expiring May 18, 2009.
- Privacy Impact Assessment approved on March 22, 2006, expiring March 22, 2009.

CFOL:

- C&A approved on May 18, 2006, expiring May 18, 2009.
- Privacy Impact Assessment approved on March 22, 2006, expiring March 22, 2009.

SAAS:

- C&A approved on June 12, 2007, expiring June 12, 2010.
- Privacy Impact Assessment approved on January 22, 2007, expiring January 22, 2010.

IRFOF:

- C&A is currently in process.
- Privacy Impact Assessment is currently in process.

OPA (it should be noted that OPA is also referred to as eIA):

- C&A approved on June 13, 2007, expiring June 13, 2010.
- Privacy Impact Assessment approved on December 11, 2006, expiring December 11, 2009.

eServices:

- C&A approved on April 2, 2008, expiring April 2, 2011.
- Privacy Impact Assessment approved on April 2, 2008, expiring April 2, 2011.

12. Will other agencies provide, receive, or share data in any form with this system?

No other agencies provide, receive, or share data in any form with this system.

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

All taxpayer data is stored in IDRS and CFOL and is accessed by the MIRSA application during a user's session. Therefore, these systems are responsible for data elimination at the end of the retention period in accordance with IRS policies and procedures.

All MIRSA session data is destroyed when the user terminates his/her Web browser client; logs out of the application; or when the session timeout period of fifteen (15) minutes has elapsed due to inactivity. Data stored in the above-mentioned IRS systems is not permanently stored or maintained by the MIRSA application.

Username and passwords that are created by authenticated taxpayers and stored in the ITAS authentication database are retained in the database as long as the user's account has not been inactive for a period of fifteen (15) months. After a period of fifteen (15) months of inactivity has elapsed, a user's account is deleted and the user is required to re-register by creating a new account in order to access MIRSA. No other data beyond the taxpayer's inquiry session on the Internet is maintained except (1) unsuccessful attempts or (2) a taxpayer's request to restrict Internet access to their tax account information.

Invalid authentication attempts for Tier 1 and Tier 2 authentication are stored in the ITAS session database for the remainder of that day. Invalid authentication attempts for username/password authentication are stored in the ITAS authentication database for the remainder of that day. For both Tier 1/Tier 2 authentication and username/password authentication, at the beginning of the next day (12:00 AM Eastern Time), the ITAS subsystem executes a script that purges and overwrites the data to ensure its deletion.

Additionally, taxpayers are allowed to restrict online access to their MIRSA account through the ITAS subsystem. When a user restricts online access to their tax account, no one (including the user) can gain access to the user's tax information via the Internet. When a user restricts online access to their MIRSA account, a flag in the ITAS authentication database is updated. The taxpayer is the only person who can remove the restriction placed on their account.

14. Will this system use technology in a new way?

No. MIRSA does not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups?

No. This system will not be used to identify or locate individuals or groups. MIRSA is used as a means for individual taxpayers to view their IRS account information through the Internet.

16. Will this system provide the capability to monitor individuals or groups?

No. This system does not provide the capability to monitor individuals or groups.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently? Explain.

No. MIRSA is a self-service Web-based application that allows individual taxpayers to view their IRS account information through the Internet. The only users of MIRSA are taxpayers and all taxpayers will all be treated in the same way.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?

Yes. MIRSA directs taxpayers to a specified toll free number in the event that a condition exists on their account that may warrant resolution with the IRS or further clarification for the taxpayer.

19. If the system is Web-based, does it use persistent cookies or other tracking devices to identify Web visitors?

No. The system only uses "session-only" cookies. The session cookie is destroyed when the user terminates his/her Web browser client; logs out of the application; or when the session timeout period has elapsed due to inactivity (15 minutes), whichever occurs first.

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