**Compliance Research Initiative Tracking System (CRITS) – Privacy Impact Assessment**

**PIA Approval Date – March 12, 2009**

**Requested Operational Date – July 25, 2009**

## System Overview

The Compliance Research Initiative Tracking System (CRITS) is designed to assist the Office of Research to measure the results of Earned Income Tax Credit (EITC) and non-EITC research initiatives. It supports Research in their effort to retrieve tax information needed from Corporate Files Online (CFOL) databases to measure the impact of these initiatives. The Office of Research has extended the availability of the CRITS to organizations other than Research, such as Criminal Investigation and Taxpayer Advocate.

## System of Records Numbers

- Treasury/IRS 42.021 – Compliance Programs and Project Files
- 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*:** The CRITS data files include the following sensitive information:

- Taxpayer Identification Number (TIN)
- Taxpayer information from the Individual Return Transaction File (IRTF) and Individual Master File (IMF) databases such as: spouse name, Social Security Number (SSN) and address; dependent names and SSNs; wages, income, and profits; Earned Income Credit (EIC) data; and exemptions and deductions.
- Taxpayer information from the Business Return Transaction FILE (BRTF) and Business Master File (BMF) databases such as: Employer Identification Number (EIN), name, address, income, deductions, credits, and tax.

***B. Employee*:** Form 5081 (Information System User Registration/Change Request) Identification and Authentication (I&A) information of all CRITS users with access to the system.

***C. Audit Trail Information***: At a minimum, the following items are captured:

- User ID;
- IP Address;
- Date/time;
- Type of event; (e.g. logon/logoffs)
- File opened or closed
- Success or failure of event

***D. Other*:** None; no other sensitive information is used by the CRITS.

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

**A. IRS** - CRITS extracts data from CFOL via an MFE (multi-functional equipment) command known as Standard CFOL Access Protocol (SCAP). The data elements available via SCAP are the same as those available via individual CFOL command codes IMFOL, BMFOL, RTVUE, BRTVU, and INOLE.

**B. Taxpayer** – CRITS receives no information directly from taxpayers.

**C. Employee** - Employee data is obtained from the employee via the OL5081 application.

**D. Other Federal Agencies** - No data is obtained from any other Federal Agency.

**E. State and Local Agencies** – No data is obtained from any State or Local Agency.

**F. Other Third party Sources** - No data is obtained from any other third party source.

**3. Is each data item required for the business purpose of the system? Explain.**
Yes. The CRITS is designed to provide Research with the CFOL data that is both relevant and necessary to research and measure the EITC and non-EITC initiatives. All requests for data extract must be approved by the user's manager and the CRITS Executive.

Employee data is maintained strictly for the purpose of identification and authentication.

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

**Accuracy** - CRITS retrieves data from CFOL via Integrated Data Retrieval System (IDRS) Command Code SCAPD (SCAP download). SCAP passes a success code to CRITS when the request to CFOL is successful.

CRITS has many field validations, such as date fields, built into the Web pages In addition, CRITS enforces the use of drop down menus to ensure users select only valid values.

In addition, CRITS uses the Core Record Layout for CFOL to create the data extract, which specifies the position and length of data elements on the CFOL record.

**Timeliness** - Timeliness is satisfied by the availability of extracts on a CFOL-cycle basis (which is weekly), and by the user's ability to request extracts for any time period on an ad-hoc basis.

**Completeness** - Completeness is determined by the user by cross-validating the number of output records with input records

**5. Is there another source for the data? Explain how that source is or is not used.**
No.

**6. Generally, how will data be retrieved by the user?**
The CRITS users prepare a list of IMF, IRTF, BMF, BRTF, and/or National Accounts Profile (NAP) data elements for which they need data to complete their study (i.e. a product). After receiving approval for the data extract, the CRITS user submits a list of TINs for which they need this data. CRITS extracts the data from CFOL through the Standard CFOL Access Protocol (SCAP). The data elements available via SCAP are the same as those available via standard CFOL command codes

such as IMFOL, BMFOL, RTVUE, BRTVU, and INOLE. After the data elements are extracted, CRITS packages data for insertion into a data base and for use with statistical analysis tools. The CRITS user retrieves their data from CRITS using an https (secure http) connection. A record of the data extraction, the equivalent of a Form 6759, Request for taxpayer Data, is maintained for 7 years.

**7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?**
User must provide the TIN and Tax Period for data extraction.

**Access to the Data**

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

**User** – Researchers have access to taxpayer data as defined by the Memorandum of Understanding (MOU), and to statistical reports.

**Managers** – Managers, Project Office (PO) Administrators and the CRITS Executive will have access to approval pages, employee data, and statistical reports. They may have access to taxpayer data if they also have the role of researcher.

**CRITS 5081 Admin** – The CRITS 5081 Admin will have access to employee data for the purpose of adding, updating or deleting users.

**System Administrator/Database Administrator** – System Administrators and Data Base Administrators (SA/DBAs) will have access to taxpayer and employee data for the purpose of troubleshooting only. In such case, an Information Technology Assets Management System (ITAMS) ticket is required.

**Developers** – In general, developers have no access to taxpayer or employee data; however, they may be granted temporary access for the purposes of troubleshooting under the authority of an ITAMS. Developers may also be granted "situational access" when warranted (e.g. end of year changes or troubleshooting).

**Security Officers** – Security Officers will be responsible for reviewing audit logs in accordance with IRM 10.8.3.

**Contractors** – CRITS currently uses a contractor to perform system administration, such as installing software upgrades, patches, and implementing transmittals. The contracting SA typically does not have access to taxpayer and employee data unless he is asked to assist in troubleshooting a problem (ITAMS). The contractor has had a High Risk background check.

**9. How is access to the data by a user determined and by whom?**
A completed Form 5081 must be approved and submitted before any user will be provided access to the CRITS. The CRITS 5081 Administrator may grant the following roles:

- Researcher – An IRS employee who creates products and MOUs, submits requests, and retrieves response data.
- Manager – First level of approval for products and MOUs, authority to "sign" Form 6759, Request for Taxpayer Data, and the Taxpayer Browsing Protection Act Unauthorized Access (UNAX) agreement, and has limited ability to update their employees' user profiles (name, SEID, email address, etc).

- CRITS Project Office Administrator – Final level of approval for products and has limited ability to update the user profiles of managers and below.
- CRITS Executive - Final level of approval for MOUs, and has limited ability to update the user profiles of managers and below.
- CRITS 5081 Administrator – Ability to add, update, delete users from system. This role has no other authority.

Once authorized to access the CRITS, the user must prepare a Memorandum of Understanding (MOU) that identifies the specific tax information needed (i.e. product), the person(s) authorized to submit TINs and retrieve the response, duration of the study (i.e. start and end date), total number of extracts, total number of TINs to be submitted, and other pertinent information. The user's manager and the CRITS Executive must review and approve the MOU which grants the user permission to extract a specified number of tax records. Upon submission of a TIN file, the user's manager must also review and "sign " an Unauthorized Access (UNAX) statement that indicates they accept all UNAX responsibilities and that they agree to adhere to all security, privacy, and government standards for protection and disposal of taxpayer data.

**10. Do other IRS systems provide, receive, or share data in the system?**
Yes. Taxpayer data is received from CFOL via SCAP (Standard CFOL Access Protocol). This data is then passed on to IRS employees who have been authorized to use CRITS, such as researchers and statisticians.

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

**C&A**
IMF = 06/12/2007 (includes IMF, IRTF CFOL, and SCAP subsystems)
BMF = 06/12/2007 (includes BMF, BRTF CFOL & SCAP subsystem)
IDRS = 05/18/2006

**PIA**
IMF – 06/07/2007
BMF – 04/12/2007
IDRS – 10/31/2008

**12. Will other agencies provide, receive, or share data in any form with this system?**
No other agencies provide, receive or share data with the CRITS.

**Administrative Controls of Data**

**13. What are the procedures for eliminating the data at the end of the retention period?**
CRITS is currently unscheduled. An SF 115 was submitted to NARA proposing a 7-year retention for the records stored in the data store. Once approved, CRITS data will be destroyed in accordance with all disposal standards.

**14. Will this system use technology in a new way?**
No

**15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.**
No

**16. Will this system provide the capability to monitor individuals or groups?**
Yes. The Office of Research may use data provided by CRITS to study taxpayer behavior by analyzing the taxpayer's account before and after a treatment.

CRITS has placed the following process in place to prevent unauthorized monitoring:

1. Before an authorized user can submit a request for taxpayer data, they must identify the data elements they wish to study. This list of data elements, known as a CRITS product, must be approved by the user's manager and the CRITS PO Admin.
2. Next the user must create an MOU that outlines the project on which they are working, who is authorized to retrieve the data, and the extent of the research they want to perform (which product, how many TINs and how many times). The user's manager and the CRITS Executive must approve the MOU before a request for taxpayer data can be submitted. In addition to approving the MOU, the user's manager must also electronically sign a statement indicating that they accept responsibility for ensuring compliance with all security measures, taxpayer privacy rights, and government standards concerning the use of taxpayer data.
3. Once the MOU is approved by both the manager and CRITS Executive, the user may submit a request for taxpayer data. If the request falls within the terms of the MOU, CRITS will accept the request and create a Form 6759, Request for Taxpayer Data. The user's manager is then notified that a Form 6759 is ready for their approval. No data extraction will take place until the user's manager signs the Form 6759.
4. Once the data is extracted, only users identified on the MOU may retrieve the response file.

**17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?**
No

**18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?**
CRITS does not make negative determinations.

**19. If the system is Web-based, does it use persistent cookies or other tracking devices to identify Web visitors?**
Yes. The CRITS deletes the cookie when the user logs off or closes the browser

**View other PIAs on IRS.gov**