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

PIA Approval Date – Jan. 14, 2010

System Overview

The Compliance Research Initiative Tracking System (CRITS) is a web–based tool used primarily to evaluate the impact of Research's outreach initiatives and to extract specialized data requested by outside parties including Congress and other agencies. The application allows the user access to Business Return Transaction File On–line (BRTFOL), Individual Master File (IMF), Individual Returns Transaction File On–Line (IRTFOL), and National Account Profile (NAP) data from Corporate Files Online (CFOL). An authorized user submits an electronic request asking for the disclosure of specific tax information as outlined in the Product. Each request contains at a minimum the Taxpayer Identification Number(s) (TINs) and the number of requested years the user would like to research (up to four tax years). The authorized user will submit several TINs at one time via the Intranet using an https front end. CRITS extracts the data from CFOL using SCAP (Standard CFOL Access Protocol), a Multi–Functional Equipment (MFE) command, that provides downloads of raw data from CFOL. CRITS employs the Legacy Access Provider (LAP) to control the flow of data returned by SCAP. Upon receipt of the SCAP response, CRITS parses through the CFOL data extracting only the data the researcher has requested and discarding the remainder. CRITS formats the response data into output files that can be loaded into a database of the user's choice. This data extraction takes place behind the scenes on the application server. Once notified that their response is ready, the user has 14 days to access CRITS and retrieve the response data.

Systems of Records Notice (SORN):

- IRS 42.021--Compliance Programs and Project Files
- 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) database 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

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

A. IRS – CRITS extracts data from Corporate Files On Line (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, 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.

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 Earned Income Tax Credit (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. There is no other source for the data.

6. Generally, how will data be retrieved by the user?
The CRITS users prepare a list of IMF, IRTF, 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, Return Review (RTVUE), Business Return Transaction View (BRTVU), and Information On Line Entity (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?
Yes. A 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)?

Role: User
Permission: Researchers have access to taxpayer data as defined by the Memorandum of Understanding (MOU), and to statistical reports. Read (products) (MOUs) and write (products) (MOUs)

Role: Managers
Permission: 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.

Role: Research Manager
Permission: Read (products) (MOUs) and write (products) (MOUs)* (approvals)

Role: Project Office Administrator
Permission: Read (products) (MOUs) (delegations) and write (user profiles) (delegations) (approvals)

Role: CRITS Executive
Permission: Read and write (user profiles) (delegations) (approvals)

Role: CRITS 5081 Admin
Permission: The CRITS 5081 Admin will have access to employee data for the purpose of adding, updating or deleting users. Read and write (approvals) (products) (MOUs) (expire user's access)*

Role: System Administrator/Database Administrator
Permission: 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. Read, write, delete

Role: Developers
Permission: 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). Read (only in development), write (only in development), delete (only in development)

Role: Security Officers
Permission: Security Officers will be responsible for reviewing audit logs in accordance with IRM 10.8.3. Read access.

**Note: User has the ability to expire products and MOUs but they cannot delete them from the system.*

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? If YES, list the system(s) and describe which data is shared.
Yes. CRITS retrieves taxpayer data from CFOL via Integrated Data Retrieval System (IDRS) Command Code SCAPD (SCAP download) part of IMF and BMF. SCAP passes a success code to CRITS when the request to CFOL is successful. 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?

Individual Master File (IMF)

- Certification & Accreditation (C&A) – June 12, 2007 (includes IMF, IRTF CFOL, and SCAP subsystems)
- Privacy Impact Assessment (PIA) – June 07, 2007

Business Master File (IMF)

- Certification & Accreditation (C&A) – June 12, 2007 (includes BMF, BRTF CFOL & SCAP subsystems)
- Privacy Impact Assessment (PIA) – April 12, 2007

Integrated Data Retrieval System (IDRS)

- Certification & Accreditation (C&A) – May 18, 2006
- Privacy Impact Assessment (PIA) – October 31, 2008

12. Will other agencies provide, receive, or share data in any form with this system?
No. 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?
The National Archives and Records Administration provided a signed SF 115, citing IRM 1.15.22 that approved a 7–year retention period for the records stored in the CRITS database.

14. Will this system use technology in a new way?
No. CRITS does not use technology in a new way.

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
No. CRITS is not used to identify or locate individuals or groups.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
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 Project Office Administrator.
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. CRITS does not allow IRS to treat taxpayers, employees, or others differently.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
No. 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. CRITS does not employ any other tracking devices to identify web visitors.

View other PIAs on IRS.gov