Qualifying Therapeutic Discovery Grant/Credit Program Project (QTDG/CPP) – Privacy Impact Assessment

PIA Approval Date – May 28, 2010

System Overview

The Affordable Care Act creates tax credits and grants for businesses with no more than 250 full–time and part–time employees that are engaged in pursuing certain types of medical innovation. The law allows up to $1 billion total in tax credits and grants for projects that receive a certification. Updated Privacy Impact Assessments will be published as this system refines its processes.

Systems of Records Number(s) (SORN):

The system operates under the SORN Treasury/IRS 24.046 Customer Account Data Engine (CADE) Business Master file. That system covers business returns and information returns that are sent to IRS. An additional new system of records notice that more specifically describes these records and clarifies their content is under consideration.

- IRS 34.037--IRS Audit Trail and Security Records System covers records that track unauthorized access to the system

Data in the System

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

A. Taxpayer Information from Form 8942)
- Primary Taxpayer Name
- Employee Identification Number (EIN)/Taxpayer Identification Number (TIN)/Social Security Number(SSN)
- Address
- Secondary Taxpayer Name (DBA)
- EIN/TIN/SSN
- Address
- Third Party Taxpayer Name (Power of Attorney)
  - (Not capturing third party EIN/TIN/SSN)
- Address
- Various field from various forms such as:
  - Sensitive But Unclassified (PII) identifying data such as Name, SSN, EIN, ITIN, Address, City, State, Zip code.
  - Data from forms 1120, 1065, 1040, 3800, 3468.
- IRS Systems:
  - Business Master File (BMF)
  - Individual Master File (IMF) Returns Transaction File

Note: the IRS is in the process of determining all the IRS forms and systems with which we will utilize data. An updated PIA will be published at that time.

B. IRS Employee:
   - Name
   - Title/Position
   - Grade
   - Work Address
   - City
   - State
   - Zip Code
   - Work Phone number
   - Group number
   - The user’s logon, pages visited, queries submitted will be recorded in the same fashion as when accessing IDRS for the audit trail.

C. Audit Trail – Access privileges within the system is granted based on job function need and is authorized by appropriate IRS management via Form 5081, Information System User Registration/Change Request. The system the user uses collects employee login information. SharePoint activity will also collect various user information e.g., the user's E–Mail address, Date of activity (add/edit), Data accessed, Data changed, Data added. SharePoint database will be certified secure at all time and for all users.

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

A. IRS – Sensitive But Unclassified (PII) identifying data such as:
   - Name
   - SSN
   - EIN
   - ITIN
   - Address
   - City
   - State
   - Zip code
   - Data from forms 1120, 1065, 1040, 3800, 3468
   - IRS Systems, BMF, IMF, RTF.

B. Taxpayer – The original source for tax return information is the taxpayer via filed returns, which are processed electronically, transcribed, or captured though various action or transaction codes on the form or in the system.

C. IRS Employee – IRS employees who use the system:
   - Name
   - User Name
   - Title/Position
   - Grade
   - Work Address
   - City
   - State
   - Zip Code
   - Work Phone number

- Group number

D. Other Federal Agencies – Health and Human Services

3. Is each data item required for the business purpose of the system? Explain.
Yes, each data item is necessary to perform a required business action (add, edit, update etc.). Data will provide a means to identify areas of non–compliance. Using this information, available efforts can be focused on the more significant potential non–compliance issues and to validate the recipients of the credit were in fact approved to receive the credit.

4. How will each data item be verified for accuracy, timeliness, and completeness?
The data will come primarily from IRS Systems – Authoritative Sources. It is expected most of files are pre–processed using existing methods of verification by the IRS function responsible for it. Any additional information through user input is verified through programming to trap errors before the item is submitted. The timeliness and accuracy of the information is again reviewed during classification and case building before assignment.

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 front–end process will be an access database that will be housed on SharePoint where authorized users can add, edit, view and download information in summary or by specific records for use in determining compliance. The data retrieval and validation process has not been clearly defined at this time – but is expected to be data derived from IMF, BMF and other data sources – the methodology is still in the development phase.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. The taxpayer's EIN and SSN information is going to be retrievable in the system. The EIN document retrieval is the primary expectation though the use of an SSN taxpayer documents may also be used, we anticipate users will also have the ability to enter a name, address, filter (a set of selection criteria), etc., any of which give the user a TIN which can then be referenced to access the tax return. At this juncture it is not planned to retrieve information by a personal identifier of a user of the system – though we are in the process of developing our requirements and working with Cybe–Security to determine the development of the audit trail. However it will be common practice for a user to retrieve records and identify another user that has added those records or are Program Coordinator.

<u>Access to the Data</u>

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
The Access Database develop/programmer, IRS users, managers, System Administrators, Database Administrators. Access will not be permitted except as authorized by law. The data is protected by the confidentiality requirements of section 6103 of the Internal Revenue Code.

Note: No outside contractors will have access.

9. How is access to the data by a user determined and by whom?
Access to the data is determined by the the confidentiality provisions of the Internal Revenue Code.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s).

- Business Master File (BMF)
- Individual Master File (IMF)
- Modernized Electronic Filing (MeF)
- Code and Edit
- Electronic Filing (E–File)
- Account Management System (AMS)
- Integrated Production Model (IPM)

This system is in the development stage. We are in the process of determining all the IRS systems with which we will retrieve data, and which data elements will be shared.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
Any Systems that will provide data or receive data, will have had an approved Authority to Operate (ATO) and hold an approved Privacy Impact Assessment.

12. Will other agencies provide, receive, or share data in any form with this system?
The Health and Human Services (HHS) will provide the IRS information with regard to the taxpayer being awarded a grant or credit through this initiative. The IRS will share data with HHS to the extent authorized by law

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?
IRS and NARA Record Retention Policies and Procedures will be followed for the data retention and elimination. Generally, records will be disposed of in accordance with the Records Disposition Handbook for Compliance programs and projects. Normally, return information is kept for a 5 year period. The Business Owner is working with the IRS Records Office to determine the precise record retention schedule for this effort. When approved, the Record Control Schedule will be published in a revised Privacy Impact Assessment.

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.
The records will only be used to identify or locate applicants as needed to administer the law. Its only purpose is to ensure compliance with the Grant/Credit Program and general tax compliance.

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.
No. Its only purpose is to ensure compliance with the Grant/Credit Program and general tax compliance.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. Its only purpose is to ensure compliance with the Grant/Credit Program and general tax compliance. All users of the system will be required to follow National Office documents, including the

IRM, Examination Plan, directives, and memoranda, which lead to consistent use of the data and avoid disparate treatment of individuals or groups.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
The database is being developed to track incoming material to then validate and send to HHS when authorized by law. HHS will then make a determination on those that are qualified for a grant/credit. The purpose of this system is to allow us to track these activities and then allow the IRS to ensure compliance and identify fraudulent activities by combining various data elements with the front end Access Database. This system of records may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual. This system of records may not be accessed for purposes of inspection or for contest of content of records. 26 U.S.C. 7852(e) prohibits Privacy Act amendment of tax records.

19. If the system is web–based, does it use persistent cookies or other tracking devices to identify web visitors?
The system is not expected to be web–based, and will not be available to outside sources. It is expected to track the users through SharePoint Access Control, a secure site within the IRS.

View other PIAs on IRS.gov