NOTE: The following reflects the information entered in the PIAMS Website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: 06/10/2014 PIA ID Number: **1014**

1. What type of system is this? Legacy

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

Health Coverage Tax Credit Program-Closeout Phase, HCTC

2a. Has the name of the system changed? Yes

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

Health Coverage Tax Credit Program (HCTC)

3. Identify how many individuals the system contains information on

Number of Employees:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	100,000 - 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

The HCTC Program facilitated the implementation of the legislatively mandated health coverage tax credit through the Trade Adjustment Assistance Act. The HCTC Program was not reauthorized by Congress and expired January 1, 2014. The program is now in the process of closing out its existing system. Since HCTC Business Operations must support post HCTC system shutdown tasks, it will be necessary to transition the HCTC reporting database and managed library into the IRS from the contractor site. The IRS will maintain the new RICS database at the IRS MCC. The types of data maintained in the reporting database that will be transitioned include participant, health plan, financial, and eligibility. By standing up an internal IRS database, providing the required tools, access, and SQL SME support, the IRS HCTC analysts will be able to research historical data as needed. The reporting database is read only and no new data will be collected. This will allow the analysts to make accurate decisions on returned funds, eligibility issues, corrections to master file notching, and other ad hoc inquires or requests received from external stakeholders. IRS HCTC will maintain spreadsheets of manual returned funds and eligibility updates. These work products will be stored on the HCTC server. The HCTC Program received lists of individuals who were potentially eligible for the health coverage tax credit from the State Workforce Agencies (SWA), through the Interstate Connection Network (ICON), and from the Pension Benefit Guaranty Corporation (PBGC). Starting January 1, 2014, HCTC only received backdated eligibility data on existing HCTC participants prior to 2014. The Program no longer accepted backdated eligibility data systematically after April 15, 2014. From this date on, HCTC will receive updates via IRS electronic fax from SWAs and PBGC. All HCTC systems and sites maintained by contractors were closed on or before June 20, 2014. IRS HCTC will continue to work with US Bank to process any funds returned by Health Plans or individuals until the work is exhausted. All system data has been archived with the IRS Tape Library under a 10 year disposal plan. All paper documents have been archived with the National Records Center under separate disposal plans based on the type of document. The reporting database and work products will be maintained for 10 years as well and then disposed of according to record retention guidelines. Due process is provided for the HCTC pursuant to 26 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) Yes

6a. If Yes, please indicate the date the latest PIA was approved: 05/18/2010

6b. If Yes, please indicate which of the following changes occurred to require this update.

- **System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes)** Yes

- **System is undergoing Security Assessment and Authorization** No

6c. State any changes that have occurred to the system since the last PIA

The existing HCTC system has been eliminated. For post shutdown activities, a read only reporting databases has been created and stored at the Martinsburg Computing Center for IRS HCTC analysts to use for research. New data collected will be received manually and tracked in spreadsheets indicating action taken and resolution.

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	Yes	
Employees/Personnel/HR Systems	No	
Other	Yes	*Other Source:* Federal Agency (PBGC); State Agency (ICON); Third Party (US Bank, State Qualified Plans, Vendors)

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	No
Social Security Number (SSN)	Yes	Yes	No
Tax Payer ID Number (TIN)	No	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

PII Name	On Public?	On Employee?
Date of Death	Yes	No
Date of Divorce	Yes	No
Telephone	Yes	No
Gender	Yes	No
Dependent Name	Yes	No
Dependent SSN	Yes	No
Dependent Gender	Yes	No

Dependent Date of Birth	Yes	No
Dependent Relationship	Yes	No
Account Number	Yes	No
Dependent Health Plan Name	Yes	No
TP Health Plan Name	Yes	No
TP Premium	Yes	No
TP Language Preference	Yes	No
TP Access Needs	Yes	No
TP Access Notes	Yes	No
TP County of Residence	Yes	No
TP State of Residence	Yes	No
TP Secondary Telephone	Yes	No
TP HP Federally Funded Portion	Yes	No
TP Positive Eligibility Checkbox from Self-Attesta	Yes	No
Employee Assigned User ID	No	Yes
Vendor Name	Yes	No
Vendor EIN	Yes	No
Vendor Address	Yes	No
Vendor POC Name	Yes	No
Vendor Telephone	Yes	No
Vendor Date Added in System	Yes	No
Vendor Payment Remittance Information	Yes	No
TP Group ID	Yes	No
TP Member ID	Yes	No
TP Policy ID	Yes	No
Updated Date of Birth	Yes	No
TP Coverage Type	Yes	No
TP OT Exception Amount	Yes	No

10a. Briefly describe the PII available in the system referred to in question 10 above.

Taxpayer data in the reporting database includes, the customer account number, SSN, date of birth (DOB), updated DOB, date of death, date of divorce, address, gender, dependent information (name, SSN, gender, DOB, relationship, health plan), vendor information (health plan, third party administrator, employer group), policy information (member ID, group ID, policy ID, coverage type, premium, OT amount (dental/vision)), language preference, access needs, access notes, county of residence, state of residence, primary and secondary phone number and secondary phone number, federally funded health plans the individual participated in. Only data elements that were required to process the monthly HCTC credit option for individuals or qualified family members and reimbursement credits for HCTC, according to the Trade Adjustment Act (TAA) guidelines are maintained. There is no Employee data in the system. Limited IRS HCTC employees have access to the reporting database for post shutdown work. IRS HCTC employees will be authenticated to the database using their IRS SEID. A paper 5081 will be maintained for approved access to the database. Audit trail information in the system: The Audit Trail will capture the user ID of any individual that accesses the reporting database server. No alterations are permitted. Vendor data in the system includes vendor name, employee identification number (EIN), address, point of contact name, phone number, date of entry and payment remittance information. Vendors are health plans, third party administrators, or employers (e.g., Health Plan of the DC Metro Area).

If you answered Yes to Social Security Number (SSN) in question 10, answer 10b, 10c, and 10d.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

SORN: Treasury/IRS 22.012-Health Coverage Tax Credit Program Records Public Law 107-210, The Trade Act of 2002 - Credit for Health Insurance Costs of Eligible Individuals Public Law 111-05, American Recovery and Reinvestment Act (ARRA) of 2009 Public Law 112-40, Trade Adjustment Assistance Extension Act of 2011 (TAA Reauthorization)

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

Customer account number is an auto-generated account number within the system that will be used whenever possible to limit the use of SSNs.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

The auto-generated account number is in place. No other strategies are planned.

11. Describe in detail the system's Audit Trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an Audit Trail is not needed.

Audit Trail information in the system: The Audit Trail will capture the SEID, date and timestamp of any system user that accesses the database. No alternation of the data is permitted. The system users will be a limited number of IRS HCTC employees. In order to access the database, SQL Server Manager Studio (SSMS) is required. Users are limited to a set of stored procedures to search for the information required to conduct their research. Work products created from data queries will be stored on the same server as the database. User privileges and user roles are limited to read only and users can only execute queries using the stored procedures.

11a. Does the audit trail contain the Audit Trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: No

If Yes, the system(s) are listed below:

No System Records found.

b. Other federal agency or agencies: Yes

If Yes, please list the agency (or agencies) below:

The HCTC reporting database will maintain data received from the Pension Benefit Guaranty Corporation(PBGC) systemically through April 15, 2014. HCTC will maintain SSN, name, address, DOB (if available), eligibility month/year, eligibility adjustment code for each eligible individual through PBGC. Beginning April 16, 2014, eligibility data will be received manually from PBGC via IRS electronic fax. This data will be maintained in spreadsheets and stored on the server.

c. State and local agency or agencies: Yes

If Yes, please list the agency (or agencies) below:

The HCTC reporting database will maintain data received from the Interstate Connection Network(ICON) systemically through April 15, 2014. HCTC will maintain SSN, name, address, DOB (If available), eligibility month/year, eligibility adjustment code for each eligible individual through a State Workforce Agency(SWA). ICON consolidated data sent by the individual SWAs. Starting April 16, 2014, eligibility data will be received directly from the SWAs via IRS electronic fax. ICON will no longer provide consolidated data. This data will be maintained in spreadsheets and stored on the server.

d. Third party sources: Yes

If yes, the third party sources that were used are:

The HCTC reporting database will maintain data received from U.S. Bank systemically through April 14, 2014. HCTC will maintain payment data received by US Bank identified by customer account number. Beginning April

15, 2014, payment data and any correspondence received by US Bank will be mailed to the IRS HCTC analysts. A spreadsheet of daily payments received will be emailed to the IRS HCTC analysts. The HCTC reporting database will maintain data received from state governments (Departments of Insurance) for State Qualified Health Plans (SQHPs) designated by the state governments. The final list of State Qualified Plans has been captured in the system. No further data will be collected or maintained after January 1, 2014. The HCTC reporting database will maintain data received from all Vendors which include Health Plan Providers, Third Party Administrators, and Employer Groups, received through January 1, 2014 and manually entered into the system. HCTC will maintain vendor name, EIN, address, point of contact name, phone number, date of entry, and payment remittance information. The final Vendor Data has been captured in the system. No further data will be collected or maintained after January 1, 2014.

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): No

g. Other: No **If Yes*, specify*:**

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

All data collected was necessary for administering the monthly HCTC, end-of-year Tax Credit, and reimbursement credit program mandate as described in the HCTC regulation. No health information was collected. The data collected will be maintained in the HCTC reporting database and used post-HCTC program closeout by HCTC analyst to have the ability to make accurate decisions on returned funds, eligibility issues, corrections to master file notching, and other ad hoc inquires or requests received from external stakeholders.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct Tax Administration	Yes	
To provide Taxpayer Services	Yes	
To collect Demographic Data	No	
For employee purposes	No	
		If other, what is the use?
Other:	No	

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	No		No
State and local agency (-ies)	No		No
Third party sources	No		No
Other:	No		

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?
If yes, please indicate means:

	YES/NO	AUTHORITY
Persistent Cookies		
Web Beacons		
Session Cookies		
Other:		*If other, specify:*

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

18a. If Yes, how is their permission granted?

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

19a. If Yes, how does the system ensure "due process"?

Denial Determinations: Denial of benefits could have occurred when or if an individual is not listed on eligibility records provided by PBGC or the SWAs. In those situations, the individual would need to contact the SWA or PBGC to have that entity determine whether there was an error in the eligibility records provided to HCTC. An individual could have been denied benefits if they failed the self-attested questions as dictated by the HCTC regulations. The process to appeal denial is below. An individual could have been denied benefits in the event that an individual did not have a qualified vendor. Enrollment in a qualified plan may have permitted enrollment in HCTC again. An individual could have been denied benefits if they either did not send in a document so that the program could verify vendor and premium amount, or if the individual did not send in their portion of the premium. There is a process for individuals to appeal denial from the monthly program. Appeal Process: Within the text of our system letters for ineligibility, we included the following text: What To Do If You Disagree: If you believe this information is incorrect, follow these steps: 1. Continue to pay your health insurance bills in full directly to your health plan. You can claim the yearly HCTC on your federal tax return for any months you were eligible for the tax credit and made direct payments to a qualified health plan. 2. Call the HCTC Customer Contact Center and have a copy of your HCTC Registration Form available. A Customer Service Representative will review the HCTC Program requirements with you. 3. If you still disagree, you will be instructed to send a letter of appeal. 4. The HCTC Program will review your appeal and respond with a decision letter.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If Yes, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If No, how was consent granted?

Written consent _____

Website Opt In or Out option _____

Published System of Records Notice in the Federal Register _____

Other: _____

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Only
Managers		No Access
System Administrators		Read Write
Developers		No Access
Contractors:	No	
Contractor Users		No Access
Contractor System Administrators		No Access
Contractor Developers		No Access
Other:	No	

If you answered yes to contractors, please answer 22a. *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have "Root Access", does that person hold a properly adjudicated "High Level"background investigation? Yes

23. How is access to the PII determined and by whom?

HCTC has identified a set of IRS employees that will have access to the reporting database. Each user is granted read only access. Form 5081 will have signatures from the User's Manager/COR, the Functional Application Manager, and the Security Administrator. The System Administrator grants user's access in the system based on the information completed on the Form 5081. Users will only be given access after Form 5081 is completed.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

All data maintained in the reporting database received from ICON and PBGC was checked for proper format at the time the data was received. The information that was received from ICON and PBGC is expected to be accurate. This includes all data that was loaded into the system through April 15, 2014. After that date, backdated eligibility records are received manually via IRS electronic fax and used to make appropriate adjustments to eligibility as needed. This data is maintained in a spreadsheet on the server. HCTC maintains a tollfree number for taxpayers to leave a voicemail. IRS analysts will manage the calls and open cases in a manual spreadsheet to track and maintain any action or resolution required. If contact with the taxpayer is required, IRS analysts will authenticate the taxpayer by confirmation of SSN, name, and address.

25. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

25a. If Yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

A SF 115 Request for Records Disposition Authority for HCTC and associated records (Job No. N1-058-09-102) was submitted to the National Archives and Records Administration (NARA) and was approved May 13, 2010. Disposition instructions for HCTC inputs, system data, outputs, paper documents and system documentation have been published in IRS Document 12990 under Records Control Schedule 18 for the Enterprise Computing Center - Detroit (DCC), item 68. All paper documents stored at the Federal Records Center follow the approved disposition schedule which includes 5, 7 and 10 year-retentions based on the type of document. A 10-year disposition has been approved for system data, including eligibility information for all potentially eligible and eligible participants. This data is stored at the IRS Tape Library, MCC. Removal of the data in storage will be handled by proper degaussing of the magnetic media used for storage, in accordance with procedures described in IRM 10.8.1. The HCTC reporting database stood up April 30, 2014. The data maintained in the reporting database will follow the 10-year disposition schedule, as well.

If No, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

The HCTC System follows FIPS PUB 200 minimum security requirements for the appropriate security controls and requirements as described in NIST SP 800-53 Revision 3. The appropriate policy checkers, network checkers, security scans, and critical updates are maintained. The technical controls that the reporting database has in place are mainly inherited from the GS. The system administrator role includes: 1) Controling remote access to the system; 2) Installing OS updates and patches; 3) Running system policy checker; 4) Ensuring the system configuration remains in compliance with the SQL server policy checker. The database administrator role includes: 1) Adding/Removing users to/from SQL server; 2) Assigning access levels to SQL server users; 3) Creating and maintaining database instances; 4) Running the SQL Server policy checker; 5) Ensuring the SQL Server configuration remains in compliance with the SQL server policy checker; 6) Backing up the data. All other administrative and technical controls are inherited by the GS. All RICS applications will be using databases housed on a SQL server using Windows authentication only. SQL Server authentication will be disabled on the SQL server to comply with IRM requirements. Database roles will be created for each database, and proper “least privilege” permissions will be assigned on all pertinent database objects (tables, stored procedures, views, etc…) to these roles. Rather than adding each application user as a login to the SQL server, we will create Local windows groups on the SQL server with appropriate names describing the application and access level within in the name (ie, Contacts_Admin and Contacts_StdUser). These local windows groups will then be added as SQL logins and given only the permission to the database needed for the application. In addition, the local windows groups will then be placed in the corresponding database role. The security administrator, based on the 5081, will place the IRS user into the appropriate local windows groups, which has already been mapped to the appropriate access level on the SQL server.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

Data At Rest: The HCTC reporting database is read only. The database has been archived on a separate drive and a separate server in the event it needs refreshed. The server is maintained under the IRS GS and controls for "Protection of Information At Rest" which outlines the configurations for firewalls, gateways, intrusion detection/prevention systems, and filtering routers are inherited. Data In Flight or In Transition: HCTC does not maintain any data in flight or in transition. SQL Server is setup to protect data. From a database level, we have enabled TDE (Transparent Data Encryption) will will encrypt the entire database’s file contents. This means that if someone were to access the MDF, LDF or BAK files associated with that database, they would not be able to read the contents by restoring or attaching those files to their own SQL server. The majority of the protection for the data will be in the permission setup. The goal is to deny most permission to the actual tables in the database, and create stored procedures to perform the bulk of the data manipulation.

For example, if I deny the DELETE permission on a table to a user, they will not be able to delete a record in that table, through an application or through SSMS. However, we can create a stored procedure that contains the code to DELETE a record, and then give EXECUTE permission on that stored procedure to that user. This provide the best level of security so that users MUST go through pre-defined methods of manipulating data.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? No

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

GS Level: System/Intrusion Detection System (IPS/IDS) and Host Intrusion Detection System (HIDS). Monitoring Roles: SAs and DBAs assign initial identifications and passwords, security profiles, and other security characteristics of new users. Other tasks include changing security profiles for existing users, ensuring that user's access or type of access is restricted to the minimum necessary to perform his/her job, and monitoring system integrity, protection levels, and security-related events. Additionally monitoring activities include running policy and network checkers and scans. System logs are maintained.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*? No

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If YES, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORNS Number	SORNS Name
22.012	Health Coverage Tax Credit Program Records
34.037	IRS Audit Trail and Security System

Comments

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	Yes
Provided viable alternatives to the use of PII within the system	Yes
New privacy measures have been considered/implemented	No
Other:	No

32a. If Yes to any of the above, please describe:

SSN Use Reduced: System users that will search for data are IRS employees. They will locate the Taxpayer's Data by searching for the taxpayer's customer account number, TIN/SSN, or name in the reporting database. The customer account number will be used whenever possible to limit the use of SSNs.

View other PIAs on IRS.gov