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: 08/21/2014 PIA ID Number: **1029**

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

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

Collection Due Process-Certified Mail System, CDP-CMS

2a. Has the name of the system changed? No

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

3. Identify how many individuals the system contains information on

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

4. Responsible Parties:

NA

5. General Business Purpose of System

The purpose of the CDP Certified Mail System (CDP-CMS) is to maintain the certified mailing information and delivery status regarding letters sent to taxpayers. This is to ensure that the correspondence has been sent so that taxpayers are not burdened by levies or garnishment due to not receiving the appropriate and adequate correspondence from IRS. The system information is used by ACS Support or Appeals when processing CDP hearing requests to confirm if a certified letter was sent to the taxpayer. The system was originally designed to automate the tracking of the mailings of USPS Forms 3811. This was required by RRA98. The CDP-CMS was implemented in 2002. In 2007 a modernized application, the CDP Certified Mail Repository (CDP-CMR) was created that replaced the Form 3811 cards with electronic file transfers between USPS and IRS. This application maintains a database repository with the status of all mailings since October 2007. The CDP-CMS database has been static since then and is accessed for reporting and research purposes on certified mailings prior to October 2007. It has a retention period of 12 years. Due process is provided 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: 04/18/2008

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

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

no changes.

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'.** none

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 Source:
Other	No	

---

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	No	No
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	No	No	No

Additional Types of PII: No

No Other PII Records found.

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

The CDP-CMS will display the taxpayer SSN/TIN, name, address and the Postal Service certified mail number.

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.)

CDP-CMS was created in response to the IRS Restructuring and Reform Act os 1998 (RRA98). IRC 6109 is the authority that allows this system to contain SSNs.

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

No changes are planned for this system. The system requires the SSN / TIN be input in order for it to pull up the information. The data in this system is static containing data for a time span limited to 2002 to 2007. The need for it's existence continues to decrease as the potential for receiving CDP cases from those years decreases.

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

The data in the system has been static since 10/2007 and there is a 12 year retention period. The system will be retired in 2019.

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.

The system does not maintain Audit Trail information specific to user IDs and passwords. It has evident driven Audit Trails such as time stamps.

11a. Does the Audit Trail contain the Audit Trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

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: No

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

c. State and local agency or agencies: No

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

d. Third party sources: No

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

e. Taxpayers (such as the 1040): No

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.

When the CDP cases are being worked by ACS Support, Appeals or Chief Counsel occasionally there will be a case where the is a need to obtain proof that a correspondence was sent to the taxpayer. The input of the TIN enables the CDP-CMS to search the database for the Postal Service certified mail number related to the correspondence in question.

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	No	
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)			
State and local agency (-ies)			
Third party sources			
Other:			

** 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”?

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due Process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

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	Yes
Other:	No

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		Read Only
System Administrators		Read Only
Developers		Read Only
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
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?

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

Users must request access by applying for approval through the OL5081 process. The user's manager must sign off on the OL5081 to grant the user access to CDP-CMS.

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

There are numerous edits and validations in place prior to data being modified in the application. Furthermore the application has several error reports that run frequently to ensure data is complete, accurate and timely. Most data entry screens are pull down menus with no options for manipulating the data.

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.

CDP-CMS data is scheduled under National Archives and Records Administration (NARA) Job No. N1-58-11-6, as approved for its successor system called the Notice Delivery System (NDS). Disposition instructions are published in Records Control Schedule (RCS) Document 12990 under RCS 29, item 39. Certified Mail Data is to be maintained for 12 years after processing year.

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 users position and need-to-know determines the type of access to the data. The ACS Support CDP Unit managers grant approval for CDP-CMS access. Users must request acces through the on-line Form 5081 process to obtain and user ID and password and are assigned to only those system permissions needed to perform their job. A users access to data determines when it is no longer needed.

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

Official use is restricted to those who have completed the 5081 process and have been issued a user ID and password.

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? Yes

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

N/A. In 2010 system was re-classified as a non-application and removed from the FISMA inventory.

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)*?

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
IRS 00.001	Correspondence Files
IRS 24.029	Individual Account Number
IRS 22.054	Subsidiary Account File
IRS 22.060	Automated Non-Master File
IRS 22.060	Automated Non-Master File
IRS 24.030	CADE Individual Master File
IRS 24.046	CADE Business Master File
IRS 34.037	IRS Audit Trail and Security

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)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No

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

NA

View other PIAs on IRS.gov