

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: 02/12/2014 PIA ID Number: 768

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

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

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

Electronic Crimes Environment, ECE

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: Under 50,000

Number of Contractors: Not Applicable

Members of the Public: Under 100,000

4. Responsible Parties:

NA

5. General Business Purpose of System

The Electronic Crimes Environment (ECE) application resides on the Electronic Crimes Technology Support Center (ECTSC) Criminal Investigation Workgroup Criminal Investigations (CI-2) GSS and provides the necessary tools to securely access and collaborate on electronic case evidence. The Electronic Crimes Environment supports Criminal Investigation (CI) core mission of serving the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law. In regard to question 19 of this PIA, ECE does not provide due process however due process is provided to the taxpayer, on what is produced from the system, form outside the system.

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: 07/20/2011

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 Yes
-

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

The system has been moved to the ECC Memphis and resides in a separate physical security cage that protects from unauthorized physical access and inherits all high system PE controls.

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'. 015-00-02-00-01-5201-00

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:

Data is received from other federal, state and local agencies as well as third parties as needed on a case-by-case basis to support an investigative need

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	Yes
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?

No No

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

Work product on case by case basis.

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.)

Title 26, tax related violations, money laundering, narcotics and counter terrorism.

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

Investigative Purposes require that these data elements be collected to support the investigation regardless of whether or not another source exists.

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

SSN are required for cases that point to an individual and is unique to the individual. There is no mitigation strategy.

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.

System administrators maintain all data in folders that have specific rights granted to each user. Logs are created to track the files viewed by each user. These logs can be used to audit the data accessed by a given user as well as provide chain of custody documentation for the resource. Audit events captured by the system Audit Logs: Logon and logoff Password changes data object access such as open and closed. Reading, editing and deletion of object files. Date and time of event. The unique identifier (user name, SEID, application name, etc.) of the user or application initiating the event.

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:

Dependent upon the case, CI-2 can receive data in the form of evidence or work products that is only available to authorized user, to their respective evidence container from the employees of another federal agency. FBI, SS, ICE, Postal, or any other federal agency could provide data in the form of work product. The work product could be case images, records, data sets, or other electronic data related to a criminal investigation.

c. State and local agency or agencies: Yes

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

Dependent upon the case, CI-2 can receive data in the form of evidence or work products from the employees of state and local agencies.

d. Third party sources: Yes

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

Dependent upon the case, CI-2 can receive data in the form of evidence or work products from other third party sources.

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.

To effectively preserve, store, analyze, and process seized data in a forensically sound manner to support criminal investigations. Provide users (Special Agents) with the necessary infrastructure to securely access and collaborate on seized evidentiary case data. Ensure that seized digital evidence is expeditiously and securely accessible. Enforcement of tax law.

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	<u>No</u>
To provide Taxpayer Services	<u>No</u>
To collect Demographic Data	<u>No</u>
For employee purposes	<u>No</u>

Other:	<u>Yes</u>
--------	------------

If other, what is the use?

Tax law enforcement

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? No

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

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	_____	No
Website Opt In or Out option	_____	No
Published System of Records Notice in the Federal Register	_____	No
Other: <u>Search warrant and subpoena's.</u>	_____	Yes

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:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Only</u>
System Administrators		<u>Read Write</u>
Developers		<u>Read Only</u>
Contractors:	<u>Yes</u>	
Contractor Users		<u>No Access</u>
Contractor System Administrators		<u>Read Write</u>
Contractor Developers		<u>Read Only</u>
Other: <u>Contract Managers</u>	<u>Yes</u>	<u>Read Only</u>

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?

CI-2 GSS is not accessible and/or available to the general public. Access to the data by a user is determined, by a combination of an EA enterprise automated system, via the EA OL5081 process, in conjunction with Criminal Investigation's internal ECMIS tool, after appropriate CI CCB and TAB boards approve the initial OL5081 to enforce physical and logical access restrictions associated with the Agents, CIS/users designated access, enforcing least privilege using the authentication via active directory.

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

The incoming data is validated for accuracy and completeness by using hashing algorithms and time stamps. When timeliness is an issue for user, the date time stamp is used to verify the time the data was created. Data is created from investigative research and receives duplicate data from law enforcement agents. The user (Agent) is responsible for ensuring that the data is accurate and complete.

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? No

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.

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.

ECE is non-recordkeeping and no other scheduling actions are required. ECE is a temporary staging area for investigative evidence to be reviewed, but it is not the official repository for any data or documents. All ECE data relating to a CI investigation will be removed/disposed of by the Lead Agent (CIS/Investigator) in accordance with Investigative Case Files under RCS 30, item 15 (soon to be moved from IRM 1.15.30 and published as RCS 30 in Document 12990). Copies of the audit logs are moved to long-term storage and are maintained as per IRM 10.8.3 After CI's consultation with Criminal Tax Counsel and the Department of Justice, CI is following the recommendation per the signed Memo, September 21, 2010 by Victor Song, initiated on September 17, 2010, for data residing on the CI-2 GSS. Electronic copies of records other than the "recordkeeping copy", will be destroyed

or deleted within 180 days after the record keeping copy has been produced. The exception is litigation holds; CI adopts a 180-day retention policy for monthly backup tapes. This retention policy is in keeping with that of IRS–MITS and resolves the growing logistical difficulties of storing the monthly backup tapes indefinitely. Moreover, because the case-related material contained on the backup tapes duplicates material that is maintained elsewhere, destruction of the tapes would not compromise our ability to comply with criminal litigation discovery requests. Following the expiration of the 180-day period, the tapes will be recycled or destroyed, in keeping with existing media destruction policy. The only exception to the proposed 180-day retention period for monthly backup tapes are situations where there is an existing litigation hold imposed by the Department of Justice, the Office of Chief Counsel, or a specific court order. The 180-day period will be suspended for backup tapes under the purview of a litigation hold. The Technology Operations & Investigative Services E-Discovery Program (EDP) is responsible for monitoring litigation holds and for notifying appropriate TOC personnel when the suspension can be lifted. Prior to recycling or destroying any tapes, the local custodian will review EDP SharePoint for any applicable litigation hold. After CI’s consultation with Criminal Tax Counsel and the Department of Justice, CI is following the recommendation per the signed Memo, September 21, 2010 by Victor Song, initiated on September 17, 2010, for data residing on the CI–2 GSS. Electronic copies of records other than the “recordkeeping copy”, will be destroyed or deleted within 180 days after the record keeping copy has been produced. The exception is litigation holds; CI adopts a 180-day retention policy for monthly backup tapes. This retention policy is in keeping with that of IRS–MITS and resolves the growing logistical difficulties of storing the monthly backup tapes indefinitely. Moreover, because the case-related material contained on the backup tapes duplicates material that is maintained elsewhere, destruction of the tapes would not compromise our ability to comply with criminal litigation discovery requests. Following the expiration of the 180-day period, the tapes will be recycled or destroyed, in keeping with existing media destruction policy. The only exception to the proposed 180-day retention period for monthly backup tapes are situations where there is an existing litigation hold imposed by the Department of Justice, the Office of Chief Counsel, or a specific court order. The 180-day period will be suspended for backup tapes under the purview of a litigation hold. The Technology Operations & Investigative Services E-Discovery Program (EDP) is responsible for monitoring litigation holds and for notifying appropriate TOC personnel when the suspension can be lifted. Prior to recycling or destroying any tapes, the local custodian will review EDP SharePoint for any applicable litigation hold.

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

Access to the system requires a background check. The only users that are able to access are current CI personnel. An OL-5081 request is required for access.

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

Hash encryption.

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.

Enterprise FISMA activity is closely followed and adhered to.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - IT Security, Live Data Protection Policy? Yes

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (if appropriate)? Yes

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted? 01/31/2012

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 24.046	Customer Account Data Engine Business Master File,
IRS 34.037	Audit Trail and Security Records System
IRS 46.009	46.009--Centralized Evaluation and Processing of I
IRS 46.005	Electronic Surveillance Files

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

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

Not Applicable.

[View other PIAs on IRS.gov](#)