

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: 6/22/15

PIA ID Number: **1374**

1. What type of system is this? Exempt Organizations Compliance Area Database, EOCA Database

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? No

If **yes**, enter the full name, acronym, and milestone of the most recent PIA.

Next, enter the **date** of the most recent PIA.

Indicate which of the following changes occurred to require this update (check all that apply).

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

Were there other system changes not listed above? _

If yes, explain what changes were made.

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

Business Purpose: The purpose of the EOCA database is to track all inventory in the Exempt Organization Compliance Area. Functionality includes identifying cycle time and hours per case for BPR purposes, detailed project tracking, generating TP Letters, Transmittals, and several operational reports. Location: Split Database - Front-end (code, application) located on laptop; Back-end (data only) located on file server in Ogden UT - ODN001BPFP2. Access to the Database: The users have a desktop icon that runs a Windows 7 script that downloads the most current copy of the Front-end to the laptop if the Front-end has been changed since the last time the user logged into the database. It also insures the laptop has the most current files (letters, forms) on the laptop which are used by the database to generate pre-populated letters. Approximate Number of Users: 55 to 60 - Averages 20 simultaneous users during work hours. Users are located in Atlanta GA, Cincinnati OH, Dallas TX, and Ogden UT. Users not in Ogden UT use Remote PC's when available to access the database.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information, any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or variations of SSN s (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or SSN variation) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

<u>No</u>	Social Security Number (SSN)
<u>Yes</u>	Employer Identification Number (EIN)
<u>No</u>	Individual Taxpayer Identification Number (ITIN)
<u>No</u>	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
<u>No</u>	Preparer Taxpayer Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or variations of SSN s).

Individual SSN's are not used within the EOCA database; EIN's are required for identification of the record. The EOCA database will eventually be migrated into the RCCMS application (PIA approved), but no timeframe for that transition has been approved at this time.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates according to Privacy Requirements? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	No	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No

No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	No	No	No
No	Live Tax Data	No	No	No

6c. Does this system contain SBU information the system that it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Letter of Understanding (LOU)	Documents that have been marked OUO or LOU
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and

		facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

<u>Yes</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>No</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>No</u>	PII for personnel administration is 5 USC
<u>No</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>No</u>	Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

Individual SSN's are not used within the EOCA database. EIN's are required for identification of the record. This Entity Information is extracted using MEF / RICS. The EOCA database will eventually be migrated into the RCCMS application (PIA approved), but no timeframe for that transition has been approved at this time.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

The organizational records are created from information extracted from MEF or RICS data extracts. This information is then imported into the EOCA database. QMF is the primary tool used to do the data extracts. The SBU/PII information exists before being stored in the EOCA database and no NEW data is created solely by the EOCA database. In other words, no EOCA database information transmits back to MEF, RICS, or any other system of record. All master file data corrections are done through established IRM manual procedures; there are no batch upload files from EOCA database to make mass changes to the master file. The EOCA Database does NOT make determinations. All determination are completed through the Examination process with no direct correlation to the EOCA database.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNS that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

<u>SORNS Number</u>	<u>SORNS Name</u>
Treas/IRS 50,222	TEGE Case Management Records
Treas/IRS 34.037	Audit Trail and Security Records

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act?

D. RESPONSIBLE PARTIES

N/A

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
BUSINESS MASTERFILE	Yes	04/24/2015	No	
MEF	Yes	12/17/2014	No	
RICS	Yes	06/02/2017	Yes	10/27/2014

11b. Does the system receive SBU/PII from other federal agency or agencies? No

Organization Name Transmission method ISA/MOU

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? No

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

17b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

The EOCA Database does NOT make determinations. All determination are completed through the Examination process with no direct correlation to the EOCA Database.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):

18b. If no, why not? The EOCA Database does NOT make determinations. All determination are completed through the Examination process with no direct correlation to the EOCA Database.

19. How does the system or business process ensure due process regarding information access, correction and redress?

The EOCA Database does NOT make determinations. All determination are completed through the Examination process with no direct correlation to the EOCA Database.

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated)

IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level(Read Only/Read Write/Administrator)</u>
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	No	

Contractor Employees? No

21a. How is access to SBU/PII determined and by whom? Job Title/Position determines ACCESS LEVEL within the database. Job Title usually ties directly to roles and permissions. MANAGER approves access level.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act?
Not Applicable

I.1 RECORDS RETENTION SCHEDULE

22. 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

22a. 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.

22b. 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.

The EOCA Database is unscheduled. A Request for Records Disposition Authority will be drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions will be published in Records Control Schedule (RCS) Document 12990 under RCS 24 for TE/GE.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? No

23a. If **yes**, what date was it completed?

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion?

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Do not know

23.1 Describe in detail the system s audit trail. The user is required to have access to the SERVER and the specific FOLDER where the EOCA database is located. This access is controlled and administered

through IT Network Services; this group is an external group. Only the database users get access to the specific EOCA database folder. The database records the last time users logged into the database, and also the prior log in as well. It also stores the computer the users logged in from. Because we back-up the databases nightly we have a history of everyone who logs into the database. We keep 20 days of back-ups, but the network servers would have files much further back, and we could always recover the files using network services. In other words, the file history would be as long as network services keep the files. A single record is created for each user based on a SEID, and a user cannot access the database without having a record in the USERINFO table. If you're not a user in the database, it prompts you to enter your information the first time, but the SEID and Computer Name comes directly from the IRS Windows Operating System. The database Access Level field defaults to the lowest level for new users; 0. The key fields are created using VBA functions that get the key pieces of information directly from the IRS Windows Operating System and not within MS ACCESS and not entered manually by the User. The fields are; SEID, LastLogin, PriorLogin, ComputerName. Each user has an ACCESS LEVEL which determines the functionality available while running the database. Some records within the database tie directly to the SEID who created them. For example, when a Chronical Case Record (CCR) is manually created to record what was done on the case, how long it took to work the case, general comments, and/or follow-up date information. Other records within the database are created AUTOMATICALLY and tie directly to the SEID who performed the action. For example, the status code is changed on the record. A HISTORY CCR is created automatically that says what the old status code was before the change, the SEID that changed it, and on what date it was changed. Other fields that change that automatically create a HISTORY CCR include; Status Code, Disposal Code, Assigned To, Project Code, Follow-up Date, Contact Type, and Tax Period.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

If **no**, please explain why. Don't know - to be determined.

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

26a. IRS Employees:	<u>Under 50,000</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>Not Applicable</u>
26d. Other:	<u>No</u>

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees or IRS contractors in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? No

End of Report
