

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: Jun 25 2014 12:00AM

PIA ID Number: **961**

1. What type of system is this? New

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

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

Enterprise Document Management Platform, EDMP

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

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

Consolidated Documentum Infrastructure

3. Identify how many individuals the system contains information on

Number of Employees: Under 50,000

Number of Contractors: Under 5,000

Members of the Public: Not Applicable

4. Responsible Parties:

NA

5. General Business Purpose of System

Enterprise Document Management Platform (EDMP) is made up of Development, Test, Production and Disaster Recovery Linux Consolidated Systems located in Enterprise Computing Center – Martinsburg (ECC-MTB) and Enterprise Computing Center – Memphis (ECC-MEM) within Enterprise Operations (EOPS). EOPS is responsible for the deployment and daily maintenance of the hardware and software configurations of EDMP's infrastructure. EDMP provides a common document management platform to support existing and proposed projects with Document and Records Management requirements. It also provides a collaborative environment that allows users to manage documents that need to be processed and stored securely in a repository. Currently a number of existing IRS systems like AMS, MEDS, RSPCC, eContracts, DocIT, Chief Counsel and CMC, use Documentum to manage their documents. EDMP would allow the IRS to realize economies of scale brought about through implementing shared content servers, DB servers, index servers and SAN. EMDP is built on a Red Hat Linux Platform.

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) No

6a. If **Yes**, please indicate the date the latest PIA was approved:

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)
 - System is undergoing Security Assessment and Authorization
-

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

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	<u>Yes</u>	
Employees/Personnel/HR Systems	<u>Yes</u>	
Other	<u>No</u>	<u>Other Source:</u>

-
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)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: No

No Other PII Records found.

-
- 10a. What is the business purpose for collecting and using the SSN?

SSNs are used for identification purposes

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.)

SSNs are permissible from Internal Revenue Code (IRC) 6109, "Identifying Numbers" which requires individual taxpayers to include their SSNs on their income tax returns.

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

SSNs are the primary key, used by auditors and analysts to tie together tax forms relating to a tax case. The replacement of this identifier with a masked ID would be not feasible.

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

NA

Describe the PII available in the system referred to in question 10 above.

EDMP is a platform that provides infrastructure support (i.e. applications that reside on EDMP) to document management applications that may contain the following types of PII information - Tax payer names, Addresses, SSNs, TINs, DOB, etc, as contained on IRS Tax forms, schedules and returns. The type of PII information is limited to the scope of projects leveraging EDMP.

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.

EDMP provides audit trail capability. EDMP tracks and maintains a log of all user activity that takes place in the system. Audit data is collected on successful login (SEID that signed in), document accessed, document created or modified, date and time accessed and workflow initiated. Each transaction is recorded in the audit tables and can be retrieved through a query.

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: Yes

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

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
SEID from Active Directory	No		No	
Other Federal and State Agencies	No		No	
SEID from Active Directory	No		No	
Other Federal and State Agencies	No		No	

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): Yes

f. Employees (such as the I-9): Yes

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

C. PURPOSE OF COLLECTION

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? Yes

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

Tax Payers have the option to decline to send information

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 affected parties the opportunity to clarify or dispute negative information that could be used against them in denying benefits or disciplinary actions.

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

Authorized users who have requested and been granted access through OL5081 and are approved by their management

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

The projects on this infrastructure have data validation checks in place. Please refer to projects PIA for details on the process involved

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.

Records on this infrastructure will be disposed of (i.e. destroyed/purged if approved as a temporary record, transferred to the National Archives and Records Administration (NARA) if approved as a permanent record) in accordance with IRS Records Control Schedules/General Records Schedules (RCS 8-37 published in Document 12990, and GRS 38-64 published in Document 12829). Recordkeeping series using this infrastructure and identified as unscheduled are to be scheduled in coordination with the IRS Records and Information Management (RIM) Program Office.

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.

Documentum's security model allows projects to define groups, roles and access controls with privileges for accessing content.

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

Documentum security has plug-ins for tokens, biometrics and certificates and can be validated in real time against LDAP directories. Uses SSL encryption for communication and prevents eavesdropping security breaches. Documentum's Information Rights Management Services protects documents after retrieval from the repository. And in addition to this Documentum's Trusted Content Services enforces security based on rules and requirements

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.

Monitoring will be performed by Admin to ensure that security plan controls are functioning as expected. Please refer to projects for details on this.

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

Treasury/IRS 00.001 Correspondence Files

Treasury/IRS 34.037 IRS Audit Trail and Security Records System

Treasury/IRS 36.003 General Personnel Records

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:

N/A