Date of Approval: March 11, 2019 PIA ID Number: 3787

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Enterprise Document Management Platform, EDMP

2. Is this a new system? No

2.a. If no, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

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

EDMP PIA 1579

Enter the approval date of the most recent PCLIA. 12/18/2015

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

No Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
No Conversions
No Anonymous to Non-Anonymous
No Significant System Management Changes
No Significant Merging with Another System
No New Access by IRS employees or Members of the Public
No Addition of Commercial Data / Sources
No New Interagency Use
No Internal Flow or Collection
Yes Expiring PCLIA

Were there other system changes not listed above? No

3. What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym. Data Strategy Governance Board (DSGB)

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

Yes Vision & Strategy/Milestone 0
Yes Project Initiation/Milestone 1
Yes Domain Architecture/Milestone 2
Yes Preliminary Design/Milestone 3
Yes Detailed Design/Milestone 4A
Yes System Development/Milestone 4B
Yes System Deployment/Milestone 5
No 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.
Enterprise Document Management Platform (EDMP) is made up of Development, Test, Production and Disaster Recovery Linux Consolidated Systems 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 Account Management Services (AMS), Modified EO-EP Determination System (MEDS), Remittance Strategy for Paper Check Conversion (RSPCC), Electronic Contracts (eContracts), Documentation Control for IT (DocIT), Office of the Chief Counsel (Chief Counsel) and Content Management and Collaboration (CMC), use Documentum to manage their documents. EDMP would allow the IRS to realize economies of scale brought about through implementing shared content servers, Database (DB) servers, index servers and Storage Area Network (SAN). EMDP is built on a Red Hat Linux Platform.

B. PII DETAIL

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

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

If yes, check all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
No	Employer Identification Number (EIN)
Yes	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No	Security background investigations
No	Interfaces with external entities that require the SSN
Yes	Legal/statutory basis (e.g. where collection is expressly required by statute)
No	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	Delivery of governmental benefits, privileges, and services
No	Law enforcement and intelligence purposes
No	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

Collects and stores tax forms that have SSNs on them.

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

There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed. There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system.

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? Yes

If yes, specify the information.

Selected	PII Element
Yes	Name
Yes	Mailing address
Yes	Phone Numbers
Yes	E-mail Address
Yes	Date of Birth
No	Place of Birth
No	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
Yes	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
Yes	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
Yes	Tax Account Information
Yes	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If yes, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	Procurement sensitive data	Contract proposals, bids, etc.
Yes	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
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.

6.d. Are there other types of SBU/PII used in the system? Yes

If yes, describe the other types of SBU/PII that are applicable to this system.

Power of Attorney (POA).: name, address, telephone number, userid (User Identification), Centralized Authorization File (CAF), business address, business name, city, state, zip code, e-mail address; Tax Practitioner: Name and address; Reporting Agent File (RAF): IRS Reporting Agent Name; Return Refund Check Processing System; Taxpayer Identification Number (TIN); Taxpayer Telephone number; Transcript data Taxpayer Address; Employer Identification Number (EIN); Module data: transaction record, tax period, received date for case; Issue codes: reason for filing the case, dollar amount owed, interest, penalty, payment amount, refund amount, balance due amount, history for taxpayer advocate services users only; Employer name; Employer address; Employer Telephone Number; Business Name and Address; Business Telephone Number; Correspondence Information (Type of correspondence and date); History Information (Type of contact, resolution of address change and date); Financial Information (Bank name/address/telephone number, routing number, name of the account holder, account number, real estate, assets, wage and levy sources); Type of Tax, (e.g. Form 1040; Form 941; etc.); Filing Status; Business Operating Indicator; Entity data (i.e., taxpayer name, Tax Identification Number (TIN), address, date of birth (DOB), filing status, home phone number, business phone number); Process codes; Adjusted gross income (AGI); Itemized deductions or standard deductions; Taxable income; Affordable Care Act (ACA) Exemption Number; ACA Policy Number; and ACA Exemption Certificate Number (ECN).

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

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

6.f. 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 tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The systems and projects that reside on EDMPs platform may collect and store documents that contain PII data. EDMP will provide the platform for document management requirements. The type of PII information is limited to the scope of projects leveraging EDMP. The collection of PII data is based on specific project requirements and will be contained within the projects application. SSNs are used for identification purposes and is also limited to the scope of projects leveraging EDMP. Some of the applications residing on EDMP will assist taxpayers with tax account services and tax compliance matters. Taxpayer Identification Numbers are required to provide this service. The scope of the Account Management Services (AMS) project is to provide IRS employees with applications enabling on-demand user access and management of taxpayer accounts. IRS' account management process spans the lifecycle of a taxpayer account, from establishment of a new account, through periodic updates, posting of payments, reconciliation of deposits, account adjustments, and settlements.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

The projects on this infrastructure have data validation checks in place. They do not collect data from outside sources. Projects provide several valid checks on data that is entered into their system. Each set of data that is required is checked to ensure that all the required data is entered correctly. Additionally, projects provide validation of information entered into their systems by displaying screen indicators to notify users that more information is necessary, or data is entered incorrectly. For example, when the taxpayer information is entered, (i.e., name, address) the system checks for valid character and numeric data when displaying and during input.

C. PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

9. Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information. Yes

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

SORNS Number	SORNS Name
IRS 00.001	Correspondence Files and Correspondence Control Files
IRS 34.037	Audit Trail and Security Records System
IRS 36.003	General Personnel and Payroll Records

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

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

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

If yes, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Automated Collection System (ACS)	Yes	10/03/2018	Yes	11/20/2018
Integrated Data Retrieval System (IDRS)	Yes	03/13/2018	Yes	01/17/2018
Automated Trust Fund Recovery Program (ATFR)	Yes	02/16/2017	Yes	05/31/2017
Online 5081 (OL5081)	Yes	07/17/2018	Yes	06/14/2018

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

11.c. Does the system receive SBU/PII from State or local agencies? No

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

11.e. Does the system receive SBU/PII from Taxpayer forms? Yes

If yes, identify the forms.

Form Number	Form Name
1023	Application for Recognition of Exemption Under Section 501(c)(3) of the Internal Revenue Code
1023-EZ	Streamlined Application for Recognition of Exemption Under Section 501(c)(3) of the Internal Revenue
1024	Application for Recognition of Exemption Under Section 501(a) for Determination Under Section 120
1028	Application for Recognition of Exemption Under Section 521 of the Internal Revenue Code
4461	Application for Approval of Master or Prototype or Volume Submitter Defined Contribution Plans
4461A	Application for Approval of Master or Prototype or Volume Submitter Defined Benefit Plan
4461B	Application for Approval of Master or Prototype or Volume Submitter Plans
5300	Application for Determination for Employee Benefit Plan (Info Copy Only)
5300 Schedule Q	Elective Determination Requests
5307	Application for Determination for Adopters of Master or Prototype or Volume Submitter Plans
5309	Application for Determination of Employee Stock Ownership Plan
5310	Application for Determination Upon Termination (Info Copy Only)
5310A	Notice of Plan Merger or Consolidation, Spinoff, or Transfer of Plan Assets or Liabilities
5316	Application for Group or Pooled Trust Ruling
6088	Distributable Benefits From Employee Pension Benefit Plans
8940	Request for Miscellaneous Determination
2848	Power of Attorney and Declaration of Representative
8821	Tax Information Authorization

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

F. DISSEMINATION OF PII

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, global position system (GPS), biometrics, Radio Frequency Identification (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 (or is) notice provided to the individual prior to collection of information? Yes

17.a. 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?
EDMP is a platform that provides infrastructure support (i.e. applications that reside on EDMP) to document management applications. Verification and notification is provided by the projects leveraging EDMP. Due Process is provided pursuant to Title 5 of the Unites States Code (5 USC).

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? Yes

18.a. If yes, describe the mechanism by which individuals indicate their consent choice(s):
All individuals have the right to decline to provide information. However, they may be subject to Examination or Deficiency procedures, at which time they are provided applicable notices, such as Your Appeals Rights and How to Prepare a Protest.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them in denying benefits or disciplinary actions. Due Process is provided pursuant to 5 USC. The process and procedures are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process.

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

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

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read-Only	High
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	High
Contractor Developers	Yes	Read-Only	High

21.a. How is access to SBU/PII determined and by whom? EDMP utilizes the IRS On–Line application OL-5081 application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access via IRS OL5081 to their local management for approval consideration. Users are not permitted access without a signed 5081 form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the OL5081 form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Management monitors system access and removes permissions when individuals no longer require access. Users are assigned to specific modules of the application and specific roles within the modules and accounts follow the principle of least privilege which provide them the least amount of access to PII data that is required to perform their business function after receiving appropriate approval.

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? Yes

22.a. 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.

All records housed in the system will be erased, purged, destroyed, or transferred from the system at the conclusion of their retention period(s) as required under IRM 1.15.6, and in accordance with IRS Records Control Schedule (RCS) 19 and Document 12829 (GRS) 4.3. 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 and the IRS Records Officer.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? Yes

23.a. If yes, what date was it completed? 03/02/2015

23.1 Describe in detail the system's audit trail. 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a If yes, was the test plan completed? Yes

24.a.1. If yes, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? EDMP System Test results were captured and stored in a repository on SharePoint. Documentation shows test cases and scripts used to perform test and a pass and fail criteria to determine if requirements are satisfied

24.a.2. If yes, were all the Privacy Requirements successfully tested? Yes

24.a.3. If yes, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? 1. Accountability - Roles, Access Controls, Monitoring, Auditing and Reporting capabilities were tested. Roles - The system owner role, an admin role and a regular user roles were created. EDMP SAT-TC-01 and TC-02 test cases verified that the system owner role created during installation had rights to create the admin user and assign rights. Admin user logged in, verified and validated privileges by creating regular users, cabinets and folders. Regular user logged in, verified and

validated privileges by creating and importing documents, checked it in and out, and upload to folders. Access Control- Regular user access to repository was verified and validated by user only able to access specific repository. Error message was displayed if user attempted to access a restricted repository. Item level access was also verified and validated by testing user access to a document that the user did not have rights to view. Monitoring, Auditing and Reporting - By default the monitoring and auditing feature is turned on. Audit report was generated to verify and validate user activity involved with creation of document, check in and check out and import to folder. 2. Purpose Limitation - Internal Use and Information Sharing with Third Parties. Verified and validated that System Owner, Admin and Regular user are not able to access EDMP outside the IRS domain. "Can't reach this page error message" obtain when any user tries to access from outside IRS network. Third Party information sharing restriction tested and validated by checking ensuring that vendors do not have IRS Domain accounts, reviewing and verifying that vendors are not included in EDMPs OL5081 accounts and validating that no application accounts are created for vendors or other third parties. 3. Minimization of Collection, Use, Retention, and Disclosure - Projects on EDMP will manage and maintain the use, collection, retention and disclosure of their PII data. EDMP provides the environment and capabilities for this to take place. No PII data is used for testing purposes. Dummy data is used for testing purposes. 4. Openness and Consent - Verification and notification is provided by the projects that reside on EDMP. Tax payers have the option to decline sending information that they do not consent to. Due process is provided pursuant to 5 USC. 5. Strict Confidentiality - user access to restricted information was verified and validated by testing access to restricted repository, cabinet, folders and files. Request to access restricted areas failed for user who does not have access to restricted area and passed for user with access to restricted area. Audit reports were generated to show failed and passed access requests. 6. Security - Access control was verified and validated by testing access to restricted repository, cabinet, folder and document. User without access was unable to view item requested. Unauthorized modification and destructions were verified and validated through an audit trail query. 7. Data Quality - Projects on EDMP will manage and maintain the integrity of the data that they collect and use. 8. Verification and Notification - Verification and notification is provided by the projects that reside on EDMP. Tax payers have the option to decline sending information that they do not consent to. Due process is provided pursuant to 5 USC. 9. Access, Correction and Redress - Assigned user access and modification of data was verified and validated by testing user access to files assigned and editing of content. Modified data was verified through an audit trial query and version control. Projects on EDMP manage redress mechanisms through their business processes. 10. Privacy Awareness and Training - EDMP team completed 2018 Privacy, Information Protection and Disclosure Refresher mandatory training, Information Systems Security Refresher training and UNAX Awareness training to increase and enhance the teams awareness to designing and developing systems that would meet the training required for handling personally identifiable information. Project that reside on EDMP are also required to take the above named mandatory training.

K. SBU Data Use

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

L. NUMBER AND CATEGORY OF PII RECORDS

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

26.a. IRS Employees:	Not Applicable
26.b. Contractors:	Under 5,000
26.c. Members of the Public:	100,000 to 1,000,000
26.d. Other:	No

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 Recommendations of the 9/11 Commission 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

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees 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