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: March 23, 2016 PIA ID Number: **779**

1. What type of system is this?

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

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

Electronic Web Publication, EWord

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

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:	Under 100,000

4. Responsible Parties: *Redacted Information for Official Use Only

5. General Business Purpose of System

The business purpose of eWord is to enable the Service to fulfill its obligation under IRC section 6110 to make certain written determinations are publicly available.

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

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'. 015-000000008 Counsel Automated Legal Systems (CALS)

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

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

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Login ID	No	Yes
Name	No	Yes
Email Address	No	Yes
Docket Number	Yes	Yes
Vehicle Identifiers	Yes	No
SEID	No	No
Financial Account Numbers	Yes	No
Mailing Address	Yes	No
Criminal History	No	No
Phone Numbers	Yes	No
Medical Information	Yes	No
Place of Birth	No	No
Mother's Maiden Name	No	No
IP Addresses	Yes	No

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

The PII information flagged above is embedded in the body of Microsoft Word documents submitted by Counsel attorneys as written determinations required to be released to the public pursuant to § 6110.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

http://www.irs.gov/pub/irs-wd/00-0075.pdf http://www.law.cornell.edu/uscode/text/26/6109 Section 7801 and 7803 of the Internal Revenue Code. Collection of information that is contained in written determination is necessary to carry out the requirements of the Internal Revenue Code. Specifically, to comply with the requirement under section 6110 to make written determinations public. If a written determination contains a SSN, the SSN must be collected as part of the written determination. The SSN will be redacted before release to the public.

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

The PII information flagged above is embedded in the body of files that have been scanned & OCR-enhanced by the U.S Tax Court and officially served on the Commissioner of the IRS each business day. These documents are filed with the Tax Court by petitioners or their counsel. IRS Counsel has no control over the content of the documents.

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

The PII information flagged above is embedded in the body of files that have been scanned & OCR-enhanced by the U.S Tax Court and officially served on the Commissioner of the IRS each business day. These documents are filed with the Tax Court by petitioners or their counsel. IRS Counsel has no control over the content of the documents.

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.

At the middle tier, information is captured on the history tab, such as: the information of who logs on and the time the individuals log onto the system. Database Tier: Database auditing is configured and audit records are captured for the following activities in all three systems: use of database system privileges; statements which create, alter, delete, or rename database objects or users; session connections and failures including the usage of invalid passwords or user account, and the audit of privileged user (SYSDBA) operations. The audit trail is protected from unauthorized access. The system does not audit changes to application data including select, insert, update, or delete activities.

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
b. Other federal agency or agencies: No
c. State and local agency or agencies: No
d. Third party sources: No
e. Taxpayers (such as the 1040): <IRS.B.5.E/>
f. Employees (such as the I-9): Yes
g. Other: No

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.

The PII in eWord is collected to enable the Service to fulfill its obligation to make certain written determinations available to the public as provided by IRC section 6110. The PII is necessary to perform the legal analysis required to answer the legal question that is the subject of the written determination. We are legally obligated to make certain written determination available to the public under IRC section 6110. Regarding PII, only taxpayer identifying information is redaction as provided by statute.

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	Yes	
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

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? No

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

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. Due process is provided pursuant to 5 U.S.C.

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

20b. If **No**, how was consent granted?

Written consent	Yes
Website Opt In or Out option	No
Published System of Records Notice in the Federal Register	No
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

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Write
Managers		Read Only
System Administrators		Read Write
Developers		Read Write
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?

The access is determined by a OL5081 submitted by the requester through the business and the System Administrator.

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

This is done by the business when they do their annual review. Any PII would be verified before the documents are received as part of drafting the specific document.

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.

eWord Publication copies of written determinations are maintained for ease of reference, and may be deleted when no longer needed by Counsel. Official recordkeeping copies are maintained in Counsel physical, hard copy files.

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. The users will have to submit an OL5081 in order to grant access to the system. All users have been restricted for delete access to this system. Only CC:PA:LPD:DLS Managers and the Tester have DELETE permissions, and only for documents being processed in the WIP\6110 Documents\ sub-folders). The data was protected by using encryption backup daily. The CC-1 SSP provides the technical controls implemented at the infrastructure level.

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

Documentum security protects the confidentiality and integrity of information at rest through physical and logical security measures. The server is in the secure area with a lock and it’s also required PIV access level to get thru. There is no external access for this system. Active directory domain permissions provide logical security protection mechanisms. Encryption is used for backups that are shipped out to a remote storage location.”

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.

Testing is conducted annually to ensure the selected controls are functioning correctly. When testing of a security control reveals that the control is not functioning as expected, the control deficiency is documented in the system's plan of action and milestones (POA&M). All test results are documented and reported to Business Unit (BU) Security Project Management Office (PMO). The security state of the application is then reported to the appropriate organizational officials annually as defined in Treasury Directives Policy (TDP) 85-01.29. 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)*? No

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.

SORN Number	SORN Name
SORN ID: 82 Number: 24.030	Individual Master File (CADE)
SORN ID: 83 Number: 26.046	Business Master File
SORN ID: 84 Number: 34.037	Audit Trail and Security Records System

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: See below	Yes

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

IT has prepared and submitted the required forms to gain approval from the Office of Chief Counsel for the use of “live” data in the eWord DEV environments. Until the use of such data is approved by Counsel and the IRS Privacy Office, IT has suspended the use of live data whenever testing any system upgrades or fixes deployed into the eWord environment.