Date of Approval: **April 04, 2019**

PIA ID Number: **3977**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Electronic Web Publication, eWord

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Electronic Web Publication, eWord, PIA # 779

What is the approval date of the most recent PCLIA?

3/23/2016

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

There is no formal governance board or Executive Steering Committee for this system.

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

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

No

General Business Purpose

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.

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.
c) Exemptions from disclosure Before making any written determination or background file document open or available to public inspection under subsection (a), the Secretary shall delete-
(1) the names, addresses, and other identifying details of the person to whom the written determination pertains and of any other person, other than a person with respect to whom a notation is made under subsection (d)(1), identified in the written determination or any background file document;
(2) information specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy, and which is in fact properly classified pursuant to such Executive order;
(3) information specifically exempted from disclosure by any statute (other than this title) which is applicable to the Internal Revenue Service;
(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
(5) information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
(6) information contained in or related to examination, operating, or condition reports prepared by, or on behalf of, or for use of an agency responsible for the regulation or supervision of financial institutions; and
(7) geological and geophysical information and data, including maps, concerning wells.
The Secretary shall determine the appropriate extent of such deletions and, except in the case of intentional or willful disregard of this subsection, shall not be required to make such deletions (nor be liable for failure to make deletions) unless the Secretary has agreed to such deletions or has been ordered by a court (in a proceeding under subsection (f)(3)) to make such deletions.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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.)?

No

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

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Place of Birth

Mother's Maiden Name

Criminal History

Financial Account Numbers

Employment Information

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List (SBUList)

Proprietary data - Business information that does not belong to the IRS

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

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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.

Documents are submitted to the system by authoring individuals, and any PII contents are redacted and purged before being made public. Final documents are published at: https://apps.irs.gov/app/picklist/list/writtenDeterminations.html

How is the SBU/PII verified for accuracy, timeliness and completion?

The document content endures multiple stages of reviews. Employees are responsible for ensuring the accuracy, timeliness and completeness of any SBU/PII data they redact as part of their IRS job/duties.

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.

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

Identify the Privacy Act SORN(s) that cover these records.

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 34.037 Audit Trail and Security Records System

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

For Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

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.

This is a process by law. Notice, consent and due process are provided pursuant to 5 USC.

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

No

Why not?

The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that “taxpayers must file a return or statement with IRS for any tax they are liable for". Their response is mandatory under these sections.

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

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.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Only

Managers: Read Write

System Administrators: Administrator

Developers: Read Only

How is access to SBU/PII determined and by whom?

Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user to be added. They must submit the request via the Online 5081 process to request access to the System.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

All records housed in the system will be erased or purged from the system in accordance with approved retention periods. It is not the official repository for data and documents and does not require National Archives approval to affect data disposition. The official record keeping system for Section 6110 Chief Counsel Advice is properly scheduled under Records Control Schedule (RCS) 14 for Associate Chief Counsel, Item 5, and housed for public

inspection under the IRS Written Determination page on IRS.gov, as scheduled under Records Control Schedule (RCS) 17 for Information Technology, Item 25, 2(a).

SA&A OR ASCA

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

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

In the current application database, audit trailing is implemented. IRM 10.8.1 require auditing processes on each table and event. This auditing will include capturing the following: insert date and time, inserted by, update date and time, updated by. The data that eWord receives is from internal IRS systems which are deemed reliable and the data is validated for accuracy by the system sending the data as described in that system's PCLIA. eWord Check is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

All the customer configurable security controls are implemented as intended and documented in the eWord System documentation. They are stored on an internal office shared drive.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

Redaction and purging of sensitive data has been thoroughly tested.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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