Date of Approval: **January 27, 2023**

PIA ID Number: **7561**

SYSTEM DESCRIPTION

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

e-trak Case and Correspondence Management System, CCMS

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?

e-trak Case and Correspondence Management System, CCMS, ID #4791, MS: Operations & Maintenance

What is the approval date of the most recent PCLIA?

3/23/2020

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.

Application Development (AD)Compliance Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

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

Yes

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 e-trak Case and Correspondence Management System (CCMS) application tracks, manages and reports information relative to tax practitioners with possible Circular 230 violations, and correspondence received by Office of Professional Responsibility (OPR). Employees input new case and correspondence information into the application and update the events and actions as they occur. Reports can also be generated for this information. Due process is provided pursuant to titles 26, 18, and 31.

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.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Legal/statutory basis (e.g., where collection is expressly required by statute)

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

The CCMS program requires the use of SSN's because no other identifier can be used to uniquely identify a tax practitioner at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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

The Office of Management and Budget memorandum Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The CCMS program requires the use of SSN's because no other identifier can be used to uniquely identify a tax practitioner at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

Employer Identification Number

Other Taxpayer Identification Number

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
Standard Employee Identifier (SEID)
Criminal History
Certificate or License Numbers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

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:

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?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Federal Tax Information - Business and individual practitioners identity (name, ssn, ein, address, ptin, Date of birth, email address, telephone numbers); income (compliance issues and verify filing requirements); and IDRS transcripts (return information, tax liability). This may include clients of the practitioner (tax returns, collection information statements, status of accounts if in Collection, Offer-in-Compromise or Exam) to assist in the investigation of the practitioner's conduct. Other PII is names of employees for e-trak CCMS time reporting feature, which was added to captures data based on employee's name, case or correspondence number of cases, activity conducted, and amount of time reported and date of activity.

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)

SSN for tax returns and return information is Internal Revenue Code Section 6109

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.

SSNs of individuals and EINs of companies are used as a unique identifier of the tax practitioner that has been referred to OPR for potential investigation. SSN and/or EINs of taxpayers are sometimes reflected on referral and/or supporting case documentation that is uploaded to CCMS, but not input as data in the CCMS database. This information is found in supporting documents attached to the case electronically. Client or taxpayer information is not added to the database for easy identification and can only be accessed within the case by opening the document that was electronically uploaded/attached to the specific case. Practitioner's employer information, professional license information, and contact information such as address, fax number, phone number, and email may be input as data. Documents containing the practitioner's tax compliance history and/or authorized representation history may also be uploaded as supporting case documentation.

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

OPR uses other IRS tax administrative systems to verify and/or obtain information about a tax practitioner. There are internal programming consistency checks and record counts to validate the data that is loaded into the various IRS systems. The data that e-Trak CCMS receives is from internal IRS systems, which are deemed reliable, and the data validated for accuracy by the system sending the data as described in that system's PCLIA. Any determinations made are validated during the investigative process and the tax practitioner has an opportunity to respond to allegations.

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 34.037 Audit Trail and Security Records

IRS 37.007 Practitioner Disciplinary Records

IRS 90.001 Chief Counsel Management Information System Records

IRS 10.008 Certified Professional Employer Organizations

IRS 00.001 Correspondence Files and Correspondence Control Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

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

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: No

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

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: Form 8484
Form Name: Suspected Practitioner Misconduct Report

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

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.

Information is not collected directly from the individual. Information is provided to OPR by the referral organization or taxpayer who is submitting a complaint.

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

No

Why not?

Information is not collected directly from the individual. Information is provided to OPR by the referral organization or taxpayer who is submitting a complaint. The information collected is necessary for investigating the referral/complaint.

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

The entire process and procedures are dictated by the Internal Revenue Manual guidelines. 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 USC.

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 Write

Managers: Read Write

System Administrators: Administrator

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

The etrak CCMS system utilizes the IRS Business Entitlement Access Request System (BEARS) 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 BEARS to their local management for approval consideration. Users are not permitted access without a signed BEARS from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the BEARS 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 and System Administrators monitor system access and removes permissions when individuals no longer require access.

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 CCMS system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records

generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedule (RCS)INTERNAL REVENUE SERVICE RECORDS CONTROL SCHEDULE (RCS) 11 for IRS TAX PRACTITIONER ENROLLMENT, PROFESSIONAL RESPONSIBILITY, AND AGENT PRACTICES, Item 1 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

SA&A OR ASCA

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

Yes

What date was it completed?

10/25/2022

Describe the system's audit trail.

e-trak CCMS application has full audit trail capabilities. The audit trail assures that those who use e-trak CCMS only have permission to view and use the modules their role allows. The e-trak CCMS Systems Analyst (SA) and Information Technology (IT) Management and Program Analyst, prepares and reviews monitoring reports based on Identity Theft and Incident Management (ITIM) established timeframes. e-trak CCMS regularly runs audits to determine accounts that no longer need access to PII or are inactive. Per Internal Revenue Manual (IRM) 10.8.1.4.1.1, after 60 days of inactivity, the user's account will be disabled, but not removed from the system. After 120 days of inactivity, the account will be automatically deleted. In addition, the e-trak CCMS is reviewed annually during continuous monitoring initiatives and updated at least every three years or whenever there are significant changes to the system.

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)?

The plans are stored in DocIT and Collaborate Lifecycle Management (CLM) Quality Manager Tool.

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?

Create test cases and test scripts for security and privacy requirements. These test cases and test scripts are to validate and verify user access control procedures, ensure strict confidentiality, use of data, and accountability. In addition, e-Trak system is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (eCM) (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

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