Date of Approval: **April 06, 2020**

PIA ID Number: **4715**

SYSTEM DESCRIPTION

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

E-trak Civil Rights Division, E-trak CRD

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 Civil Rights Division (CRD) PCLIA 2198

What is the approval date of the most recent PCLIA?

3/15/2017

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

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

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 electronic CRD (Civil Rights Division) will provide the Equity, Diversity and Inclusion (EDI) organization with the ability to track complaint review processing from intake to closure. This process includes review of settlement agreements and decisions from the Equal Employment Opportunity Commission (EEOC) and Courts under Title VII, as well as Taxpayer complaints received from Treasury or the individual Taxpayer. The EEOC requires as part of its Model Equal Employment Opportunity (EEO) Program elements, that the agency maintains an automated system to track complaints, case information, and allows sharing of records between offices that EDI relies upon, for coordination and reporting (i.e. Executive Misconduct Unit (EMU), Employee Conduct and Compliance Office (ECCO), General Legal Services and Department of Treasury). Due process regarding outcomes is provided pursuant to Titles 5 and 7.

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

Standard Employee Identifier (SEID)

Employment 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

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

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.

Taxpayer complaints received from Treasury and case information. Form 14652 Civil Rights Complaint Employee complaint case information

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)

PII for personnel administration is 5 USC

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.

Names and email addresses are used to identify the individual employee or taxpayer and is only used to review the case file. This information is entered into E-Trak, which could include employee complaint (Title 6.) which could also need their date of birth and possible employment information (Title 7). Information can be added manually if needed by accessing the Treasury I Complaints (for Settlement Agreements) or Alerts systems as needed. Special access is given to employees as needed. No SSNs are used in case files to identify employees or taxpayers.

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

PII is used to identify the individual employee or taxpayer and is only used to review the case file. There are internal programming consistency checks and a record count to validate the data that is loaded into the e-trak CRD system is accurate. The data that e-trak CRD receives is from internal IRS systems which are deemed reliable. The data is validated for accuracy by the system sending the data as described in that system's PCLIA. Any determinations made are validated during Section 1203(b)(3)(B) case review process and the taxpayer/employee has appeal rights/due process for any determinations made from the data as appropriate.

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 36.001 Appeals, Grievances and Complaints Records

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?

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: F 14652 Form Name: Civil Rights Complaint

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?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

No official notice is sent to taxpayers however, taxpayers and employees are briefed on the process in accordance with Title VI and Title VII as appropriate. Employees are covered under legal and/or contractual grievance procedures and taxpayers and employees alike are asked for information to establish a case file used to process their allegations during intake with an IRS Equal Employment Opportunity (EEO) or Civil Rights Specialist. Taxpayers and employees are informed of the impact of not providing information (limited ability to investigate issues) if the issue arises during the intake process.

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

If a taxpayer or employee elects not to enter into a formal process EEO, Civil Rights complaint etc. then the information provided will not be used or shared. Employees in the EEO process complete an intake form and taxpayers correspond with a Specialist during email and or phone correspondence. Both provide written or oral consent during the intake process.

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

All data is used specifically for the process which the taxpayer or employee are involved. If a case review results in a determination of potential EEO related misconduct, all employees have the right to due process regarding information access, any corrections, and redress in accordance with IRM Guidelines.

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

Developers: Administrator

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

Users are assigned to specific modules of the application and specific roles within the modules. Accounts follow the principle of least privilege which provides them the least amount of access to PII data that is required to perform their business function after appropriate approval. The e-trak CRD system utilizes the IRS On-line OL5081 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 OL5081 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.

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.

Records are held three years in accordance with guidelines for EEO related files. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. It is the official repository for data and documents and has National Archives approval to affect data disposition and will be destroyed using IRS General Records Schedule (GRS) 1, Item 25 for EEO Records and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. GRS 2.3 Item 010-Employee relations programs' administrative records-Destroy when 3 years old, but longer retention is authorized if required for business use.

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?

12/12/2019

Describe the system's audit trail.

e-trak CRD application has full audit trail capabilities. The audit trail assures that those who use e-trak CRD only have permission to view and use the modules their role allows. The audit log events are captured in the database. All account access to the system is granted

through the OL5081 authorization process thus ensuring that authorization is granted from appropriate designated officials and that identifiers are securely distributed to the individuals requesting access. E-trak regularly runs audits to determine accounts that no longer need access to PII or are inactive. Per IRM 10.8.1.5.1.3, after 120 days of inactivity, the user's account will be disabled, but not removed from the system. After 365 days of inactivity, the account will be automatically deleted. Disabled or deleted accounts require that the user go through the OL5081 process to regain access to the system. Additionally, the System Security Plan (SSP) 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)?

In DocIt. System Test Plan, Unit Test Plan, User Acceptance testing, test cases and test scripts. The plans are stored in the DocIT repository. The test cases, test scripts and test plans are generated and stored in CLM Collaborate Lifecycle Management 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?

Test cases and test scripts were created 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. For example of testing login with valid credentials, 1) Click on the URL to e-trak CRD module using Single Sign-On (SSO),2) System should automatically put you on the landing page (Tracking inbox); 3) User role should be displayed on the upper right hand corner next to user's SEID according to the

OL5081 approval. To validate and verify system user accountability by ensuring roles and permissions are defined based on proper unique assignments. For example, 1) After logging into the system to case search, enter any part of case number, or First Name or Last Name, and the system will return a list of cases only assigned to the user. Then click on the case ID link in the search results listing, and system will display the specific case details screen.

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