

Date of Approval: March 15, 2017

PIA ID Number: **2198**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. e-trak Civil Rights Division, e-trak CRD

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.
e-trak Civil Rights Division, CRD, # 819, Operations and Maintenance

Next, enter the **date** of the most recent PIA. 5/14/2014

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

<u>No</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

Were there other system changes not listed above? No

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

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	Operations & Maintenance (i.e., system is currently operational)

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

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.

The electronic CRD (Civil Rights Division) or "e-trak CRD" will provide the Equity, Diversity and Inclusion (EDI) organization with the ability to track complaint review processing from intake to closure. This is an application of the Entellitrak suite that is currently used in many offices at the IRS. This process includes review of settlement agreements and decisions from the Equal Employment Opportunity Commission (EEOC) and Courts under Title VII, offices that EDI relies upon for coordination and reporting (i.e. Workforce Relations-ECCO and Executive Misconduct Unit, General Legal Services and Department of Treasury). Due process is provided pursuant to titles 5 and 7.

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

6a. 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.)? No

If **yes**, check who the SSN (or tax identification number) is collected on.

No On Primary No On Spouse No On Dependent

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
No	Name	No	No	No
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

6d. Are there other types of SBU/PII used in the system? No

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

No	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
No	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
Yes	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

6f. 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 electronic CRD (Civil Rights Division) or "e-trak CRD" will provide the Equity, Diversity and Inclusion (EDI) organization with the ability to track complaint review processing from intake to closure. This is an application of the Entellitrak suite that is currently used in many offices at the IRS. 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 EEO Program elements, that the agency maintains an automated system to track complaints, case information, and allows sharing of record between offices that EDI relies upon for coordination and reporting (i.e. Treasury Complaint Me a-Center, Workforce Relations-ECCO and Executive Misconduct Unit, General Legal Services and Department of Treasury). Due process is provided pursuant to titles 5 and 7."

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

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 and 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.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

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

<u>SORNS Number</u>	<u>SORNS Name</u>
36.001	Appeals Grievances Complaints

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

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? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

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, cloud, global position system (GPS), biometrics, 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/is notice provided to the individual prior to collection of information? Yes

17a. 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?

No official notice is sent to taxpayers however taxpayers and employees are briefed on process IAW 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 EEO or Civil Rights Specialists. 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.

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

18a. If **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.

19. 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 IAW IRM Guidelines.

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

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

Contractor Employees? No

21a. 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 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. The e-trak CRD system 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 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.

- 21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act
? Not Applicable

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

- 22a. 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.

Three years IAW 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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

- 23a. If **yes**, what date was it completed? 1/13/2017

- 23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion?

- 23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

23.1 Describe in detail 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 our 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. In addition, the SSP is reviewed annually during continuous monitoring initiatives, and updated at least every three years or whenever there are significant changes to the system."

J. PRIVACY TESTING

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

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process**, 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. 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 logged into the system, in case search, enter any part of case number or First Name or Last Name, system will return a list of cases only assigned to you, click on the case ID link in the search results listing, and system will display that specific case details screen.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? In Doctl. System Test Plan, Unit Test Plan, User Acceptance testing, test cases and test scripts. The plans are stored in the DoctlT repository. The test cases, test scripts and test plans are generated and stored in CLM Collaborate Lifecycle Management Quality Manager Tool.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

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:

26a. IRS Employees:	<u>Under 50,000</u>
26b. Contractors:	<u>Not Applicable</u>
26c. Members of the Public:	<u>Not Applicable</u>
26d. Other:	<u>No</u>

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 9/11 Commission Recommendations 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

N. ACCOUNTING OF DISCLOSURES

30. 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
