Date of Approval: July 26, 2017 PIA ID Number: **2739**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. e-Trak SS8 Application, e-Trak SS8

2. Is this a new system? Yes

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

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

Next, enter the **date** of the most recent PIA.

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

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

Were there other system changes not listed above?

If yes, explain what changes were made.

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

No	Vision & Strategy/Milestone 0
No	Project Initiation/Milestone 1
No	Domain Architecture/Milestone 2
No	Preliminary Design/Milestone 3
No	Detailed Design/Milestone 4A
Yes	System Development/Milestone 4B
No	System Deployment/Milestone 5
No	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.

Purpose of E-Trak SS8 Application is twofold: 1. Replace the current SS8ICP which has numerous risks to the agency as the system is failing. The current system was created in 1993 and is hardcode to accept specific years (1988 to 2014). Source documents are lost which makes it impossible to update or correct serious flaws. 2. The primary purpose the E-Trak SS8 is resolution and determination regarding taxes to be withheld either by an individual or by an entity, where the individual is working. This usually arises when there is confusion regarding contractor versus employee status. In the event of discrepancies between individual and entity regarding withholding of employment and/or income taxes, the individual/entity can complete IRS Form SS-8 Determination of Worker Status for Purposes of Federal Employment Taxes and Income Tax Withholding. This form can be completed manually and mailed into the IRS, or electronically. In both cases, there are no direct feeds into the SS8 application. The data from Form SS-8 is manually entered into the SS8 application by a SS8 user. The data in SS8 is then reviewed and analyzed for determination of contractor versus employee status. In the event of contractor status, an individual is liable for Self-Employment Tax (15.3%). In the event that the individual is considered an employee of the entity in question, the worker is liable for an employee's portion of Federal Insurance Contributions Act (FICA) tax (7.65%) and the firm is generally liable for employment taxes on the income under IRC section 3509, or may owe both the employer and the employee portions of FICA tax. Once a determination has been made the taxpayers receive a formal determination letter through the mail. The data stored in SS8 application contains privacy data and includes taxpayer identification number (TIN), taxpayer name, address, contact information, and information specific to their case which could contain tax data. SS8 serves as an online work environment for preparing case histories, documents, reports, and responses. The system is an information and audit referral resource for field personnel. For example, if an entity had not withheld the appropriate employment taxes on behalf of an individual in question, this entity could be referred to an IRS field auditor for a potential IRS audit. The SS8 application is not connected with any other application, and is not externally facing. The SS8 application shares data states as required by mutual agreements and with workload selection. This is information is shared by reports generated from the SS8 application. SS8 application users access the data within the SS8 application from their workstations. Users must submit a 5081 to obtain access and management approval is required.

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.)? Yes

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

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
Yes	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No	Practitioner Tax Identification Number (PTIN)

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

There is no alternative to the use of the TIN. The TIN is the significant part of the data being processed. The TIN of the worker and firm are needed to review, analysis and determine case outcome. TINS are used for internal research to ensure all filing requirements are met

by firm and worker. Additionally, a firm or worker can file more than one request. TIN are used to tie all related cases together ensuring consistent treatment for the firm and all workers. Requests are assigned case numbers and future enhancements may allow redaction of TINS on letters but not in the E-Trak SS8 Application.

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
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
No	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
Yes	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

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)

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

Documents associated with case activity containing PII and SBU data include: Taxpayer employment information including data about reporting forms, Employee name and badge number, Data on returns filed from internal systems, employment history with firm, and earnings. This information is used to determine worker classification with a specific firm or employment classification for a firm (worker versus independent contractor).

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

All information input into the system is from the SS8 form sent in by the requester. Information is verified for accuracy using internal research. If incorrect information is found for the entity (worker or firm) the requestor is notified and ask to correct the information and resubmit the request for worker classification. Information for the non-requester is verify by internal research and correct for data entry. All information stored is directly related to the work relationship between the worker and the firm.

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.

SORNS Number	SORNS Name
82 Number 24-030	Individual Master File (CADE)
83 Number 20.046	Business Master File
84 Number 34.037	Audit Trail and Security Record System

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? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? No

12b. Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? Yes

If **yes**, identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
ID 4377 AK PFD (Permanent Fund Dividend) Levy Program MOU	Data file	Yes

Identify the authority and for what purpose? There are numerous state and local entities we share information with, too many to reference in drop-down menu. However, the list was provided to Privacy Compliance personnel. Reports are generated on outcomes (employee or contractor). Reports are uploaded into specific state or local government folders on shared drives established by Privacy, Government Liaison & Disclosure Office (PGLD). PGLD determines which state or local governments receive information based on mutual agreements. Agreement pertain to tax administration for all parties.

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? 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, 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?
Notice is on the F - SS8 pertaining to both the Privacy Act and information on Disclosure. A statement on the form advising them if they do not want any of their information shared that they had the option of not completing the form or parts of the form and sending it to the IRS.

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):

A firm or worker may choose not to submit any additional information requested or not to complete the form.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The SS8 process and procedures are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. Information can only be accessed by IRS auditors with a need to know. Employees with access acquire access through the 5081 system approvals.

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

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

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	Yes	Administrator	Moderate

21a. How is access to SBU/PII determined and by whom? Access is obtained through the 5081-approval system. Management determines access based on need. A potential user must submit a request for access via IRS On Line (OL) 5081 to their local management for approval consideration. Users are not permitted access without a signed 5081 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. 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. Additionally, 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. 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.

SS8 data associated with Form SS-8 Determination of Worker Status for Purposes of Federal Employment Taxes and Income Tax Withholding is approved for destruction after 15 years under NARA Job No. NC1-58-79-6, and published in IRS Records Control Schedule (RCS) Document 12990 under RCS 23 for Tax Administration - Examination, Item 61. However, in reviewing SS8ICP-related recordkeeping practices for completion of this PIA, system owners and the IRS Records Office determined that a re-evaluation of final disposition instructions is in order. SB/SE and the Records Office will work together to validate and potentially update dispositions for determination of worker status to better fit current data collection activities and maintenance needs, and the current electronic recordkeeping environment. The procedures for eliminating the electronic data at the end of the retention period are found in Internal Revenue Manuals (IRM) 1.15.2 Types of Records and Their Lifecycles, 1.15.3 Disposing of Records, and 1.15.6 Managing Electronic Records. Information ages off (is deleted from) the database at varying intervals, no less than 15 years.

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

23.1 Describe in detail the system s audit trail. Data at rest is stored securely at the database layer of the database server. E-Trak protects data at rest as follows: E-Trak, in accordance with the IRM IRM 10.8.1.5.6, has employed the following due diligence methods for protecting data at rest that resides on the servers: E-Trak does not utilize any shares or shared drives. E-Trak enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties. E-Trak reports are printed in accordance with business need. Reports are handled appropriately in accordance with organizational policies. E-Trak has had a risk assessment conducted. Security Assessment Services has completed a Security Impact Analysis as part of the current SA&A cycle. The e-Trak SSP is being updated as part of the current SA&A to reflect the encryption utilized by the application to protect SBU data. Physical security is an inherited for e-Trak at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan. Within our security accreditation, the protection of data at rest is inherited from Security Control (SC) - 28: Protection of Information At Rest. The GSSs MITS-24,

MITS-30 and MITS-32 inherit the responsible for ensuring the information system protects the confidentiality and integrity of information at rest.

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.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? System Test Plan, Unit test Plan, User Acceptance testing, test cases and test scripts. The plans are stored in DocIT. 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:	Not Applicable
26b. Contractors:	Under 5,000
26c. Members of the Public:	Under 100,000
26d. Other:	No

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? Yes

    If **yes**, does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact *Disclosure* to determine if an accounting is required. Yes

End of Report