Date of Approval: **March 11, 2019**

PIA ID Number: **3894**

## SYSTEM DESCRIPTION

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

e-Trak Safeguards, SFG

*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 Safeguards, SFG 1676

*What is the approval date of the most recent PCLIA?*

3/18/2016

*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.*

Privacy, Governmental Liaison & Disclosure (PGLD) Governance Board

*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?*

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 Safeguards system provides means to the Office of Safeguards to capture, track, and manage external stakeholder statutory reporting work items and internal stakeholder work items related to Safeguards program delivery. The Safeguards Program and staff are responsible for ensuring that federal, state and local agencies receiving federal tax information protect it as if the information remained in IRS's hands. Safeguards generally accomplishes this through receipt and evaluation of required regular report submissions from agency partners as well as on-site visits to agency partners to validate and document physical and logical protections described in the report submissions and when necessary to recommend and track corrective actions when physical and logical protections for federal tax information (FTI) are found to be deficient or nonexistent. e-Trak Safeguards tool is to track cases of deficient physical and logical protections for federal tax information (FTI). E-trak is a system based on MicroPact's entellitrak, a commercial off the shelf software (COTS) product. The e-Trak Safeguards tool help to satisfy the data and functional needs of case management and metrics reporting on a more robust, web-based platform.

## 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:*

Another compelling reason for collecting the SSN

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

Taxpayer and/or employee SSNs are not collected or entered as a specific data element into the e-Trak application; however, taxpayer SSNs and FEINs are found on copies of Transcript Delivery System (TDS) access logs and analysis work papers created and stored within a Safeguard Review case. There is no alternative to the use of the SSNs or FEINs. The SSN is the significant part of the data processed via TDS which is retrieved by a state/local or federal agency and is reported to Safeguards as an attachment to justify protection of Federal Tax Information (FTI).

*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 planned mitigation strategy to mitigate or eliminate the use of the SSN or FEIN on the system.

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

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*

Proprietary data Business information that does not belong to the IRS

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities

*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.*

Copies of Transcript Delivery System (TDS) access logs and analysis work papers created and stored within a Safeguard Review case.

*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.*

Taxpayer and/or employee SSNs are not collected or entered as a specific data element into the e-Trak application; however, taxpayer SSNs and FEINs are found on copies of Transcript Delivery System (TDS) access logs and analysis workpapers created and stored within a Safeguard Review case to document the scope of the on-site reviews performed by the Office of Safeguards for external agencies that receive federal tax information (FTI). SSNs and/or ITINs reflected in the logs are based on requests for FTI by external agencies and so those reflected on the TDS logs and analysis workpapers are likely those of adult return filers but could possibly include children. The FEINs reflected in the logs are based on requests for FTI by external agencies and so those reflected on the TDS logs and analysis workpapers are likely those of business return filers (i.e. sole proprietors, corporations, s-corporations, partnerships). As part of the prep materials for Safeguards review, they receive information

regarding the FTI an agency received which would include logs of accesses to the IRS Transcript Delivery System (TDS). The logs which contain names and SSNs, would likely be included as part of the prep material for an SRR (Safeguards Review Case) case but not necessarily. PII is possible to be included as an attached document to case but not always.

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

Not verified since SSNs and TINs are not collected as a data element of the application but are reflected only on copies of Transcript Delivery System (TDS) logs which are analyzed and stored for use in Safeguard Review case related to data security reviews of external agencies that receive federal tax information (FTI).

## 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 36.003 General Personnel and Payroll 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?*

Yes

*Enter the files and databases:*

System Name: Transcript Delivery System
Current PCLIA: Yes
Approval Date: 12/3/2015
SA&A: No

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

Yes

*For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).*

Name: DOT = Department of Transportation CS = Child Support HS = Human Services DOC = Department of Corrections FED = Federal IRS = Internal Revenue Service FFM = Federally Facilitated Marketplace HSÂ¬-ACA = Human Services Affordable Care Act
Transmission Method: Email or Secure Data Transfer
ISA/MOU: Yes

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

Yes

*for each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).*

Organization Name: DOR = Department of Revenue SWA = State Workforce Agency SWA-TOP = State Workforce Agency Treasury Offset Program AG = Attorney General CS = Child Support HS = Human Services DOC = Department of Corrections CDC = Consolidated Data Center SBM = State Based Marketplace HSÂ¬-ACA = Human Services Affordable Care Act
Transmission Method: E-mail or Secure Data Transfer
ISA/MOU Yes

*Does the system receive SBU/PII from other sources?*

No

*Does the system receive SBU/PII from Taxpayer forms?*

No

*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.*

The information is not collected directly from individuals. The information collected by state/local or federal agencies is obtained via TDS and subsequently provided to Safeguards to justify protection of Federal Tax Information (FTI). Notice, consent and due process are provided via TDS and its related tax forms and instructions, and 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 information is not collected directly from individuals. The information collected by state/local or federal agencies is obtained via TDS and subsequently provided to Safeguards to justify protection of Federal Tax Information (FTI). Notice, consent and due process are provided via TDS and its related tax forms and instructions, and pursuant to 5 USC.

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

The information is not collected directly from individuals. The information collected by state/local or federal agencies is obtained via TDS and subsequently provided to Safeguards to justify protection of Federal Tax Information (FTI). Notice, consent and due process are provided via TDS and its related tax forms and instructions, and 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 Contractor 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: Read Write

*IRS Contractor Employees*

Contractor Users: Read Write

Contractor Managers: Read Write

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

A potential user will request access via the OL5081 system. This request has to be approved the potential user's manager based on a user's position and need-to-know. System Administrators of the application located in Data Services will create and assign role based user accounts to designate/control user access to PII within the application.

## 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.*

eTrak Safeguards is a COTS product that tracks the status of Safeguards reports/case files already scheduled under Job No. N1-58-00-1 and published in IRS Document 12990 under Records Control Schedule (RCS) 8, item 101. For Safeguards Procedures Reports (SPR) - destroy after 2 subsequent SPRs are received. Safeguards Activity Reports (SAR) Destroy when 5 years old. Both the SPR and SAR have been replaced by the Safeguards Security Reports (SSR) as of January 2014. SSRs will be destroyed when 5 years old. Safeguards

Review Reports - SRR (Record Copy destroy after 2 subsequent reviews are completed. Reference/Management Records are destroyed when 3 years old. Any new records identified will be scheduled in coordination with the IRS Records Officer and the RIM Office. (RIM) Program Office and submitted to the National Archives and Records Administration (NARA) for disposition approval.

## 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?*

2/24/2015

*Describe the system's audit trail.*

The e-Trak Safeguards application has full audit trail capabilities. Data files opened and closed; Specific actions, such as reading, editing; and Deleting records or fields, and printing reports. Employee and contractor transactions that add, delete, modify, or research a record. Employee and contractor transactions that add, delete, modify, or research an employee's record (personnel and financial). Employee and contractor transactions that add, delete, or modify an employee's access to e-Trak Any system transactions that alter an employee's access to e-Trak, or a system's or application's role or sub role. Any employee or contractor transactions identified by the system owner as requiring additional oversight. Any third party transactions identified by the system owner as requiring additional oversight. System, log on, log off, password change, account creation, startup, shutdown, reset, date, time, second and SEID.

## 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)?*

DocIT

*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?*

The e-Trak system is maintained by the IRS and has been approved and 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: Under 5,000

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