
A. SYSTEM DESCRIPTION

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

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 Safeguards, SFG, 399

Next, enter the **date** of the most recent PIA. 6/18/2013

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? No

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
- No System Development/Milestone 4B
- No System Deployment/Milestone 5
- Yes 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 e-Trak Safeguards system provides means to the Office of Safeguards to capture, track, and manage external stakeholder statutory reporting work items and internal stake holder 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.

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 Yes On Spouse Yes On Dependent

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

| | |
|------------|------------------------------------------------------------------|
| <u>Yes</u> | Social Security Number (SSN) |
| <u>Yes</u> | Employer Identification Number (EIN) |
| <u>Yes</u> | Individual Taxpayer Identification Number (ITIN) |
| <u>No</u> | Taxpayer Identification Number for Pending U.S. Adoptions (ATIN) |
| <u>No</u> | 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).

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). There is no planned mitigation strategy to mitigate or eliminate the use of the SSN or FEIN on the system.

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 On On

| | | <u>Primary</u> | <u>Spouse</u> | <u>Dependent</u> |
|-----|-----------------------------------------------------|----------------|---------------|------------------|
| No | Name | No | No | No |
| Yes | Mailing address | No | No | No |
| Yes | Phone Numbers | No | No | No |
| Yes | E-mail Address | No | No | No |
| No | Date of Birth | No | 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 |
| Yes | 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? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. e-Trak user's profiles contain; SEID, Grade and E-mail address.

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)
- 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.

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.

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

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).

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> |
|---------------------|---------------------------------------|
| 24.030 | IMF |
| 26.046 | BMF |
| 36.003 | General Personnel and Payroll Records |

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. *Redacted Information For Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

| <u>System Name</u> | <u>Current PIA?</u> | <u>PIA Approval Date</u> | <u>SA & A?</u> | <u>Authorization Date</u> |
|----------------------------|---------------------|--------------------------|--------------------|---------------------------|
| Transcript Delivery System | Yes | 12/03/2015 | No | |

11b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If **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).

| <u>Organization Name</u> | <u>Transmission method</u> | <u>ISA/MOU</u> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|----------------|
| DOR = Department of Revenue SWA = State Workforce Agency SWA-TOP = State Workforce Agency Treasury Offset Program DOT = Department of Transportation AG = Attorney General CS = Child Support HS = Human Services DOC = Department of Corrections CDC = Consolidated Data Center FED = Federal Internal Revenue Service SBM = State Based Marketplace FFM = Federally Facilitated Marketplace HS-ACA = Human Services Affordable Care Act | E-mail or Secure Data Transfer | Yes |

11c. Does the system receive SBU/PII from State or local agency (-ies)? Yes

If **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).

| <u>Organization Name</u> | <u>Transmission method</u> | <u>ISA/MOU</u> |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------|----------------|
| DOR = Department of Revenue SWA = State Workforce Agency SWA-TOP = State Workforce Agency Treasury Offset Program | E-mail or Secure Data Transfer | Yes |

DOT = Department of Transportation AG = Attorney General CS = Child Support HS = Human Services DOC = Department of Corrections CDC = Consolidated Data Center FED = Federal Internal Revenue Service SBM = State Based Marketplace FFM = Federally Facilitated Marketplace HS-ACA = Human Services Affordable Care Act

- 11d. Does the system receive SBU/PII from other sources? No
11e. Does the system receive SBU/PII from **Taxpayer** forms? No
11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? 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? No

17b. If **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.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18b. If **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.

19. 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.

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 Contractor 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 | Read And Write |

Contractor Employees? Yes

| <u>Contractor Employees?</u> | <u>Yes/No</u> | <u>Access Level</u> | <u>Background Invest.</u> |
|------------------------------|---------------|---------------------|---------------------------|
| Contractor Users | Yes | Read and Write | High |
| Contractor Managers | Yes | Read and Write | High |
| Contractor Sys. Admin. | No | | |
| Contractor Developers | No | | |

21a. 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. An Office of Safeguards administrator of the application will create and assign role based user accounts to designate/control user access to PII within the application.

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.

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.

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? 2/24/2015

23.1 Describe in detail 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.

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?

The e-Trak system is maintained by the IRS and has been approved and tested.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? DocIT

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: Under 50,000
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? No

End of Report
