Date of Approval: **September 26, 2022**

PIA ID Number: **7268**

SYSTEM DESCRIPTION

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

E-Trak Payroll Services, e-Trak

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 Payroll, MS4a/Ms4b. # 4394

What is the approval date of the most recent PCLIA?

10/7/2019

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.

Human Capital Office (HCO) Governance (Human Resources Information Technology)

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.

This is an umbrella all-encompassing PCLIA to describe the information in various payroll systems. As a whole, the e-trak Payroll system is a web-based application which provides a centralized database for entering and monitoring the status of different payroll related case types including Federal Erroneous Retirement Coverage Correction Act (FERCCA), Debt collection, IRS Settlement, Designated Agent, New Hire Accession Review, Military Program and Within Grade Range Increases. e-trak Payroll allows for the generation and downloading of detailed and summary reports. Reports will be used to manage cases (what has been done and when); monitor open cases by tracking the receipt of the cases (packages) sent to National Finance Center (NFC); ensuring corrections are completed and the length of time it takes for NFC to make the adjustments to retirement withholdings or Thrift Savings Plans; send letters to the affected employees; inform management of caseload per specialist; number of cases in each of workflow status; timeliness of processing cases, cycle time of processing cases, and age of cases.

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).

SSNs are required to process employee payroll retirement code fixes and updates sent to the NFC and forwarded to the Office of Personnel Management (OPM) to be finalized. OPM requires SSNs and it does not accept anything else to process the actions.

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

> The Office of Management and Budget memorandum Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record.

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
> Standard Employee Identifier (SEID)

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:

> 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.

Are there other types of SBU/PII used in the system?

> No

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

> SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

> 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.

SSNs are the only unique identifier for each employee and is used as a common key critical for accurate data validation of information.

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

PII Information for all the modules is downloaded from the Treasury-owned system Treasury Integrated Management Information System (TIMIS) and verified against employees Official Personnel Folder (OPF). Application-level and database-level completeness and validity checks are performed to ensure the data input is correct. All fields have an assigned character set, length, numerical range, acceptable values where appropriate. Input into e-trak Payroll is validated based on the e-trak Payroll business rules. A Quality Review (QR) of e-trak Payroll processing is conducted by on-site management randomly. Reporting tools used by e-trak specialists and managers are used frequently to detect mistakes in information input.

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 36.003   General Personnel and Payroll Records

IRS 34.037   Audit Trail and Security 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: e-Trak Bestrak
Current PCLIA: Yes
Approval Date: 7/13/2018
SA&A: Yes
ATO/IATO Date: 12/18/2018

System Name: Treasury Integrated Management Information System (TIMIS)
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 12/15/2018

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?

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 third-party systems of record containing the required Human Resource (HR) information is the Treasury owned Time Input Management Information System (TIMIS) system and the Treasury owned HRConnect system.

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

No

Why not?

Personally Identifiable Information (PII) for all the modules is downloaded from the Treasury-owned system TIMIS and verified against employees Official Personnel Files (OPFs).

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

Following Internal Revenue Manual (IRM) and using the automated form 5081 system called online 5081 (OL5081) and internal Quality Reviews (QRs) by separate levels of management.

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?

All new users requesting access to e-trak Payroll must do so through the BEARS system. When a user has been approved for access to the application by his/her manager, the BEARS system sends an email to the approval group, providing a notification to review and approve or deny access. Based on the user's need for access, the program managers create a user profile. The user profile contains the user's access level. Access to the application is identity and role based. Identity-Based Access Control permits access to data based on the users or owners need to access to the data. Role-Based Access Control permits access to data based on an organizational role, such as a lead or human resources assistant, which has been assigned to an individual within the organization. Users of e-trak Payroll are granted access with the most restrictive set of privileges needed to perform their duties. Security functions and sensitive information stored in e-trak Payroll is restricted to authorized personnel (e.g., security administrators). Contractors do not have access to security functions and are only assigned access level (no higher than specialist) per their assigned duties and with successfully completed interim or final National Agency Check and Inquires and Credit (NACIC) + tax background investigation granting them staff-like access to IRS facilities and systems. Currently, there are no contractors with access to e-trak Payroll.

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.

The records in e-trak Payroll and related Federal Erroneous Retirement Coverage Correction Act (FERCCA) records are scheduled under General Records Schedule (GRS) 2, Disposition Authority 'DAA-0058-2016-0016', Records Control Schedule 39, Item 23 C, and General Records Schedule (GRS) 2, for Payrolling and Pay Administration Records, Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and as coordinated with the IRS Records and Information Management Program and IRS Records Officer. Should e-trak Payroll be retired, existing data would be imported to the successor program and would be maintained in accordance with established data retention requirements for e-trak Payroll, unless otherwise updated and approved.

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?

11/9/2021

Describe the system's audit trail.

The modernized system will track employees access through system activity logs. All data entries are saved into an electronic database. The database is routinely backed up to maintain an audit trail of records as they exist when they are entered and as they are changed.

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)?

Test results stored in IT's Collaborative Lifecycle Management (CLM)repository system.

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 maintains an active IRS System Security Package (SSP) with an Authority To Operate (ATO). All testing is performed in accordance with the Federal Information Security Management Act of 2002 (FISMA). Specific testing includes but not limited to desktop walk throughs, code reviews, penetration testing etc. Specific details of the testing activities can be provided by the E-Trak testing team (IRS IT/AD compliance). As an IRS IT maintained system all testing is 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: Not Applicable

Members of the Public: Not Applicable

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?

Yes

Does your matching meet the Privacy Act definition of a matching program?

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