NOTE: The following reflects the information entered in the PIAMS website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: 9/18/14 PIA ID Number: **827**

1. What type of system is this? Modernized System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

ETRAK-Garnishment, None

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees:	Under 50,000
Number of Contractors:	Not Applicable
Members of the Public:	Under 100,000

4. Responsible Parties:

N/A

5. General Business Purpose of System

The Special Processing Office is an office that reports to the Employee Conduct and Compliance Office. The Special Process Group is responsible for processing court ordered garnishments for family support, commercial garnishments, and Chapter 13 Bankruptcies for IRS employees. They also track voluntary allotments for family support. The Special Processing Office is mandated by law to implement the garnishment process within thirty days of receipt of the legal documentation. The Special Processing Group is also required to notify the employee in writing prior to the garnishment taking effect on their paycheck. The e-Trak Garnishment module will provide the Special Process Office with an effective tool to monitor and track the garnishments. Due process is provided pursuant to 5 USC.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 12/29/2011 12:00:00 AM

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
- System is undergoing Security Assessment and Authorization No

6c. State any changes that have occurred to the system since the last PIA

PIA expired.

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. NA

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	No	
Employees/Personnel/HR Systems	Yes	
		Other Source:
Other	No	

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	No	No	No
Tax Payer ID Number (TIN)	No	No	No
Address	Yes	Yes	Yes
Date of Birth	Yes	No	Yes

Additional Types of PII: No

PII Name	On Public?	On Employee?
Phone Number	Yes	No
SEID	No	Yes

10a. What is the business purpose for collecting and using the SSN ?

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

Describe the PII available in the system referred to in question 10 above.

Data is entered into e-trak Garnishment Module by a member of the Special Processing Office. The system is password protected, and is only seen by personnel with a need to know.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Username Action Description of action(successful, or unsuccessful) URL Date of time The audit trail assures that those who use etrak Garnishment Module only see and use the modules they are allowed to use.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If **Yes**, the system(s) are listed below:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Lightweight Directory Access Protocol (LDAP)	No		No	
Outlook	No		No	
Corporate Authoritative Directory Service (CADS)	No		No	

b. Other federal agency or agencies: No

If **Yes**, please list the agency (or agencies) below:

c. State and local agency or agencies: Yes

If **Yes**, please list the agency (or agencies) below:

State Court System sends letters to the IRS when an employee is to be garnished wages. Data from this letter includes: Issuing State Court Case Number State ID Number Garnishment Type Employee Name Work Employee Address

d. Third party sources: Yes

If yes, the third party sources that were used are:

Other entities allowable by law (Banks) send letters to the IRS when an employee is to be garnished. Data from this letter includes: Issuing Entity ID Numbers Garnishment Type Employee Name Employee Address

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: No If **Yes**, *specify*:

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

Yes. Each data element is required to allow for the IRS leadership and the Business Managers to control and track the following data: The Special Process Group is responsible for processing court ordered garnishments for family support, commercial garnishments, and Chapter 13 Bankruptcies for IRS employees. They also track voluntary allotments for family support. The Special Processing Office is mandated by law to implement the garnishment process within thirty days of receipt of the legal documentation. The Special Processing Group is also required to notify the employee in writing prior to the garnishment taking effect on their paycheck.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	No	
To provide taxpayer services	No	
To collect demographic data	No	
For employee purposes	Yes	
		If other, what is the use?
Other:	No	

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) No

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)			
State and local agency (-ies)			
Third party sources			
Other:			

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?
If yes, please indicate means:

	YES/NO	**AUTHORITY**
Persistent Cookies		
Web Beacons		
Session Cookies		
		If other, specify:
Other:		

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

18a. If **Yes**, how is their permission granted?

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

IRS is required to advise the employee of the action; however, not prior to it taking place. The agency is under court order to comply so we don't have any the option to wait or stop if the employee objects. Due process would generally be provided through the court issuing the order for garnishment. See Federal Regulation Section 582.301 and Section 582.302 with regard to Garnishment.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

No forms found.

20b. If **No**, how was consent granted?

Written consent	No
Website Opt In or Out option	No
Published System of Records Notice in the Federal Register	No
Other: IRS Employee Resources Corporate Authoritative Directory Service (CADS), Lightweight Directory Access Protocol (LDAP), and Outlook are used to collect specific information about an employee to record background information about the employee	Yes

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	**Access Level**
IRS Employees:	Yes	
Users		Read Write
Managers		Read Only
System Administrators		Read Write
Developers		Read Write
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	Read Write

If you answered yes to contractors, please answer **22a.** *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have “Root Access”, does that person hold a properly adjudicated “High Level” background investigation?

23. How is access to the PII determined and by whom?

Access to e-trak Garnishment Module is determined by submitting an On-Line 5081 and receiving authorization from the user’s approval manager. The e-trak Garnishment Module application has been configured for a role-based user access policy. User access is restricted to only the specific application modules needed to complete their job function. Logical access controls have been incorporated into e-trak Garnishment Module for each user; to include assigning access privileges, session controls, and re-certification of users. Application Administrators are responsible for assigning permissions ensure that the proper permissions are granted to the proper users. All policy and procedures are followed in granting user permissions, determining permissions, ensuring user rights are restricted to the minimum necessary to perform the job, background screening and separation of duties.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

The e-trak Garnishment Module system identifies and enforces which fields are required to be completed before a record can be saved. Data validation checks are automated in the system to ensure Date Fields are valid dates,

numeric fields are numeric. The e-trak Garnishment Module has timers designed in the system that identify individual case timeliness, and is part of a management control report for monitoring.

25. 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

25a. 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.

The National archives and Records Administration (NARA) approved IRS's request for records disposition authority for garnishment case files and electronic tracking data under Job No. N1-58-09-7. IRS Employee Levy and Garnishment Case Files are approved for destruction 6 years, 3 months after end of fiscal year in which garnishment is terminated or case is closed. Tracking data of incoming documents in court-ordered garnishments for IRS employees these case files can be destroyed when 3 years old or when no longer needed for audit or operational purposes, whichever is sooner. These retention instructions are published in Document 12829 under General Records Schedule (GRS) 2/IRS Records Control Schedule (RCS) 39 for Pay rolling and Pay Administration Records, items 18b and 18c. The e-trak Garnishment Module application audit records are currently maintained for 1-year to support after the fact investigations of security incidents. The web server and application/database server auditing is managed at the MITS-24 General Support System (GSS) level. e-trak Garnishment Module follows IRS disk sanitization procedures for destruction of discarded media. IRM 2.7.4, Management of Magnetic Media (Purging of SBU Data and Destruction of Computer Media) provides those procedures used for sanitizing electronic media for reuse (e.g., overwriting) and for controlled storage, handling, or destruction of spoiled media or media that cannot be effectively sanitized for reuse (e.g., degaussing).

If **No**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
Users are assigned to specific modules of the application and specific roles within the modules and thus, only the appropriate PII data is available to those individuals to perform their duties after receiving appropriate approval and authorization through OL-5081. 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

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

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.

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? Yes

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

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.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

No SORN Records found.

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	No
New privacy measures have been considered/implemented	No
Other:	No

32a. If **Yes** to any of the above, please describe:

NA