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: 08/21/2014 PIA ID Number: **1031**

1. What type of system is this? Non-Major System

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

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

Law Enforcement eRequest System, LERS

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:	Not Applicable
Number of Contractors:	Not Applicable
Members of the Public:	100,000 - 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

This procedure allows IRS employees to go to an https site maintained by a third party (eBay Inc), log in, upload a summons and any attachments associated with that summons and return to the site and download summoned data. This improves response time and alleviates the need to send data via a less ecure method (fax/mail). IRS is not paying for eBay to create or maintain this site. Due process for the summons is provided pursuant to 26 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: 03/14/2011

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

None. In 2012, TIGTA conducted an audit of the IRS PIA process and found a number of systems/applications beyond the PIA three-year expiration date. TIGTA recommendation requires IRS to identify all completed and approved PIAs that have not been updated within three years and coordinate with system owners to review and update these PIAs as required.

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

8a. If No, what types of information does the system collect, display, store, maintain or disseminate?

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	No	
		Other Source:
Other	Yes	eBay Inc.

---

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	No
Social Security Number (SSN)	Yes	No	No
Tax Payer ID Number (TIN)	Yes	No	No
Address	Yes	No	No
Date of Birth	Yes	No	No

Additional Types of PII: No

No Other PII Records found.

10a. Briefly describe the PII available in the system referred to in question 10 above.

PII could include responsible officer's names of corporate accounts, partner names in LLCs and partnerships, spouse name, dependent name, spouse SSN, dependent SSN, addresses and phone numbers of all of the above, bank account numbers, copies of driver's licenses, web addresses.

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.)

IRC Section 7602, Examination of books and witnesses. For the purpose of ascertaining the correctness of any return, making a return where none has been made, determining the liability at law or in equity of any transferee or fiduciary of any person in respect of any internal revenue tax, or collecting any such liability. If the records in the control of the third party have TIN numbers on them, the Service is entitled to true and correct copies of those documents.

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

None. True and correct copies of documents are needed.

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

None.

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.

The IRS employee accesses the link to LERS to access an https site using their official government email. LERS then sends a confirmation email with another link to access their system (this link has a limited time-period for use). The employee again lists their official email address and confirms the challenge-response test to enter the LERS system. Once in the system the IRS employee can upload their summons document and any attachments associated with that summons. The IRS will capture its audit data from normal email traffic: the employee receiving an email from eBay and then the employee accessing the URL outside the IRS firewall. eBay employees in the fraud/legal department will have access to this system. No other employees will have access to the case.

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: No

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

No System Records found.

b. Other federal agency or agencies: No

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

c. State and local agency or agencies: No

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

d. Third party sources: Yes

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

Data received from eBay Inc on summoned customers' eBay accounts.

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.

To ascertain the correctness of any return, making a return where none has been made, determining the liability of any person for any internal revenue tax or the liability at law or in equity of any transferee or fiduciary of any person in respect of any internal revenue tax or collecting any such liability. The data received from eBay will contain personally identifiable information. The IRS will issue a summons to eBay that may be returned by eBay with the files/data honoring the summons. The summons could include identifying information to assist in identifying the taxpayer as related to an IRS case. Form 6863, Invoice and Authorization for Payment of Administrative Summons Expenses, will also contain PII.

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	Yes
To provide Taxpayer Services	No
To collect Demographic Data	No

For employee purposes	No	
		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”?

This PIA describes the process in how the third party (eBay, Inc.) will respond to us after issuing a summons. eBay is required to give us the same information they are providing us through LERS, only it would be via a CD or paper documents. The TP (or any noticee on the summons) is entitled to quash rights under IRC 7609(b). However, if the summons is a "collection" summons (i.e. issued in aid of the collection of an assessed tax), there are no "due process" rights. The TP would have the same rights through LERS as they would have if eBay responded via USPS with a CD or paper documents.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

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	
Website Opt In or Out option	
Published System of Records Notice in the Federal Register	
Other:	

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: Contractor 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 Only
Developers		No Access
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other: eBay designated employees	Yes	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?

eBay's employee access is determined by eBay employee responsibilities. IRS access is determined by IRM 1.2.52.2, Delegation Order 25-1.

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

IRS employees summon financial data for a multitude of reasons. TPs are generally asked to provide the information before a summons is issued. If there is no compliance from a TP, a summons is issued to obtain the information and/or to verify previously reported information from the TP.

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 eBay LERS system is non-recordkeeping for IRS purposes. It is a platform for secure communications and information sharing between IRS and eBay but it is not the official IRS repository for any data or documents. The

records/data secured from eBay will be downloaded from the eBay system to the IRS employee's computer and become part of the IRS employee's active case file. This data is then governed under case file criteria. The original data belongs to eBay and the IRS has no control on the retention or destruction of eBay's original data. Once the case is closed, the IRS employee will remove/delete the file from the IRS employee's computer. All case related information will be stored in a central repository and will be retained: a. for 10 years after the case is closed as required by Document 12990, Records Control Schedule (fka IRM 1.15.28), "Item 6 under Internal Revenue Service Records Control Schedule (RCS) 28, Tax Administration -- "Collection," (fka IRM 1.15.28); Item 6 b. for 10 years after the case is closed as required by Document 12990, RCS 23 for Examination (fka IRM 1.1523), Item 42; or c. for 10 years after case closed as required by IRM 1.15.30 for Criminal Investigation, Item 15 (Job No. N1-58-07-11, soon to be updated/published in Document 12990).

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.

Data will be uploaded and then downloaded from a direct transition https site to an encrypted file folder on the employee's hard drive. The employee that issued the summons will receive an email with a URL that requires them to enter their official IRS email address and the security code CAPTCHA for access into the system. This link will allow the employee to only access the file created in response to their summons. Data that needs to be saved from the summons response will be downloaded to an encrypted CD (currently the Service is employing GERS). This CD will be sent with the closed case file upon case disposition.

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

IRS employees will access the site through https links, enter their government email address and the security code CAPTCHA. The data is stored in encrypted folders on the employee's hard drive and then stored on an encrypted CD.

---

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? No

---

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

Normal case monitoring and reviews required by management to ensure employees are adhering to IT policies.

---

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.

SORNS Number	SORNS Name
Treas/IRS 24.030	IMF
Treas/IRS 24,046	BMF

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

View other PIAs on IRS.gov