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: May 25, 2016 PIA ID Number: **927**

1. What type of system is this?

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

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

Secure Object Repository, SOR

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

3. Identify how many individuals the system contains information on

Number of Employees:	Under 50,000
Number of Contractors:	Under 5,000
Members of the Public:	100,000 - 1,000,000

4. Responsible Parties: ## Redacted information for Official Use Only

5. General Business Purpose of System

Secure Object Repository (SOR) is an application designed to support requests for sensitive tax-related information by temporarily storing systemic responses to requests submitted through other internal applications that are not part of SOR. These include Taxpayers' requests handled by call assistors through Enterprise User Portal (EUP) and third party tax practitioners through Integrated Enterprise Portal (IEP). These may include, but not limited to, tax refund, tax inquiry, and copies of tax returns. In the responses, sensitive taxpayer information, such as taxpayer SSN, DOB, home address, tax returns (such as 1040), etc. are included and embedded in attached files. Tax-related information cannot be sent using ordinary e-mail to registered user and IRS employee. It has to be retained within IRS secure territory, which is SOR.

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*) No

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'. 134254045

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	Yes	
Employees/Personnel/HR Systems	No	
		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	No
Social Security Number (SSN)	Yes	Yes	Yes
Tax Payer ID Number (TIN)	Yes	Yes	No
Address	Yes	Yes	No
Date of Birth	Yes	Yes	No

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Full tax return information	Yes	No

10a. Briefly describe the PII available in the system referred to in question 10 above.
The SOR application doesn't manipulate the Personally Identifiable Information. However, the attachment saved in the Oracle database contains all kinds of return PII because it may include the taxpayer tax returns, etc.

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.)

Tax return information is used for tax administration, per 5 U.S.C.

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

SOR is not leading, but will participate in any IRS enterprise initiatives to reduce SSNs.

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

SOR is not leading, but will participate in any IRS enterprise initiatives to reduce SSNs.

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.

No information is collected on SOR side because the application debug is turned off. However, eServices side performs complete audit logging, per IRM standards.

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? No

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
Internal IRS SOR Oracle Database	No		No	
eServices	Yes	10/26/2015	No	
Employee User Portal (EUP)	No	10/26/2015	No	
Integrated Enterprise Portal (IEP)	No	10/26/2015	No	

b. Other federal agency or agencies: No

c. State and local agency or agencies: No

d. Third party sources: No

e. Taxpayers (such as the 1040): <IRS.B.5.E/>

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

g. Other: No

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.

The system is mainly used by eServices applications, such as TDS, TIN Matching, etc. The PII that is collected facilitates the IRS tax administration duty to provide taxpayers with access to their records.

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	Yes	
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.) Yes

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)	No		
State and local agency (-ies)	No		
Third party sources	Yes	Tax Practioner, CPA, etc	Yes
Other:	No		

** 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? N/A

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? Yes

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

Permission to decline to provide information is associated with the original filing of the return, as descrbed in the filing publications, such as Pub 1 and Pub 17.

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”?

SOR does not participate in due process, but supports taxpayer access to data and IRS employee ability to handle tax administration.

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.

ID	Form Number	Form Name
5874	1040	Individual tax form

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

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

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

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? Yes

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

For EUP user, the access to the PII data has to go through IRS Online 5081 process. The user has to fill out the 5081 request, and the request has to be approved by managers. After the request is approved, LDAP SA (System Administrator) adds necessary roles to the EUP user account and grants the access. For IEP users, the request is authorized through eServices eFile application to approve. Without those appropriate approvers, users cannot run the eServices applications, and retrieve and send the PII data to SOR.

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

SOR only receives and temporarily stores the PII data in SOR database. The accuracy, timelines, and completeness are all handled by eServices applications.

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.

SOR is scheduled with the National Archives under Job No. N1-58-09-43, approved 9/2/09; as published in Records Control Schedules for the IRS (RCS) 29 for Tax Administration- Wage and Investment, Item 423, a-d. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6. Any new records generated by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedules (RCS) 29, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
The PII information is usually in attachments, which are encoded and stored in Oracle database. Except the owners (EUP or IEP users), they are not visible and accessible for anyone else, such as SA or application support SME. Only database administrators, who have higher security clearance, can access.

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

The data is securely guarded in the IRS backend network through several firewalls and security software. It is very safe and secure, and guarded by Database Administrator (DBA) group. Support SMEs don't have the access to the PII data. If needed, SMEs open a format request and ask DBA to help.

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.

All user access activities are monitored and evaluated by related software or applications, such SiteMinder SSO, eServices, SAAS, and etc.

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

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.

SORN Number	SORN Name
Treas/IRS 00.001	Correspondence

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: