

Date of Approval: **May 31, 2019**

PIA ID Number: **4074**

## **SYSTEM DESCRIPTION**

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

Secure Object Repository, SOR

*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?*

Secure Object Repository, SOR, PIA # 927

*What is the approval date of the most recent PCLIA?*

5/25/2016

*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.*

Cybersecurity Privacy Management Level Governance Board

*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?*

No

## **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.*

Secure Object Repository (SOR) is an application that creates an electronic mailbox used in eServices to provide a means of storing sensitive tax-related information. Stored information includes Taxpayers' requests handled by call assistants through Enterprise User Portal (EUP) or 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.

## **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:*

Security Background Investigations

Legal/statutory basis (e.g. where collection is expressly required by statute)

When there is no reasonable alternative means for meeting business requirements

Law enforcement and intelligence purposes

*Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers)*

SOR attachments often include SSN related to the taxpayer transcripts. Many EUP and IEP users access those files.

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

This relates to the planned mitigation strategy to eliminate/mitigate the user of SSNs. The Office of Management and Budget 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. The SOR system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time.

*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

E-mail Address

Date of Birth

Standard Employee Identifier (SEID)

Financial Account Numbers

Tax Account Information

*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 (SBUList)*

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Protected Information - Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government

Criminal Investigation Information - Information concerning IRS criminal investigations or the agents conducting the investigations.

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

Yes

*Describe the other types of SBU/PII that are applicable to this system.*

Federal Tax Information - i.e., tax refund amounts, tax inquiry correspondence, etc.

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

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

Information by CI for certain money laundering cases may be 18 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.*

The SOR application doesn't manipulate the Personally Identifiable Information. However, the attachments saved in the Oracle database often contain all kinds of PII information because most are related to the taxpayer tax returns.

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

The SOR application doesn't manipulate the Personally Identifiable Information. All PII information is collected and verified by eServices applications before they are sent into SOR.

## **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 00.001 Correspondence Files and Correspondence Control Files

## **RESPONSIBLE PARTIES**

*Identify the individuals for the following system roles:*

## For 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: eServices

Current PCLIA: Yes

Approval Date: 4/20/2018

SA&A: Yes

ATO/IATO Date: 12/5/2018

System Name: Integrated Enterprise Portal (IEP)

Current PCLIA: Yes

Approval Date: 1/23/2019

SA&A: Yes

ATO/IATO Date: 5/2/2018

*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?*

Yes

*How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?*

The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number. All sensitive data is collected by eServices applications, not SOR.

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

No

*Why not?*

The legal right to ask for information is in Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. These sections state that individuals must file a return or statement with IRS for any tax for which they are liable, and response is mandatory. Notice, consent, and due process is provided pursuant to 5 USC. All these requirements are handled by eServices application, not SOR.

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

Publication 1 - "Your Rights as a Taxpayer" explains the rights of the taxpayer, which includes the right to challenge the IRS' position and be heard; and the right to appeal an IRS decision in an independent forum. Notice, consent, and due process is provided pursuant to 5 USC. All these requirements are handled by eServices application, not SOR.

## **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 Contractor Operated



*The following people have access to the system with the specified rights:*

*IRS Employees*

Users: Read Only

Managers: Read Only

System Administrators: Administrator

Developers: Read Only

*IRS Contractor Employees*

Contractor Users: Read Only

Contractor System Administrators: Read Only

Contractor Developers: Read Only

*How is access to SBU/PII determined and by whom?*

The SOR application utilizes the standard IRS on-Line access application to document approvals for access. Data access is granted on a need-to-know basis, via the Online OL5081 system.

## **RECORDS SCHEDULE**

*Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) archivist 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.*

Documents stored in this Site Collection and these sites and sub-sites are not the official records and therefore these sites and sub-sites are not considered an official recordkeeping system. The Site Owner will ensure that Site documents are appropriately destroyed/deleted when no longer needed for reference. Official recordkeeping copies are maintained in accordance with Records Control Schedule (RCS) 29, item 423 published in RCS Document 12990.

### **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?*

12/5/2018

*Describe the system's audit trail.*

SOR has a Cybersecurity approved audit plan. SOR's audit log shows failed logon attempts because either the user account-name or password is incorrect. Audit events that are application-specific are recorded in an audit trail log, transaction log and error log. Application-level audit trails monitor and log end-user activities (including administrative users). Event records specify data files opened and closed, specific actions, such as reading, editing, deleting records or fields, and printing reports, etc. SOR is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

## **PRIVACY TESTING**

*Does the system require a System Test Plan?*

No

*Please explain why:*

The system is tested whenever changes are made to the application. The SOR application hasn't been changed for several years. No additional functions have been added. SOR is currently in the Operations and Maintenance phase of its lifecycle. Continuous Monitoring (now called Annual Security Control Assessment) occurs annually to ensure that controls remain in place to properly safeguard PII.

## **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: Under 5,000

Members of the Public: 100,000 to 1,000,000

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?*

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