Date of Approval: **September 14, 2023**

PIA ID Number: **7991**

SYSTEM DESCRIPTION

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

Employee Portal (Information Returns Review), IRRP

Is this a new system?

Yes

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

This system responds to the Web Applications Governance Board, reporting to Strategic Development Executive Steering Committee ESC committee (SD-ESC).

Current ELC (Enterprise Life Cycle) Milestones:

Vision & Strategy/Milestone 0

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

System Development/Milestone 4B

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.

The Employee Portal comprises of one application with two sperate functionalities the Customer Service Representative (CSR) Portal and the Information Returns Review Portal (IRRP). The Information Returns Review Portal (IRRP) is a feature of the existing competent The Employee Portal. The Information Returns Review Portal (IRRP) is a digital portal being developed to replace in-person Submission Processing and the legacy Error Resolution System (ERS). IRRP will be used by IRS Employees who will log in using one of the following roles: Manager, Tax Examiner, and Quality Reviewer and can use this portal to complete the redress process for submissions found with forms in error. The process begins with SCRIPS, a paper-form digitization service, which sends digitized submissions to IRIS. IRIS then validates the form data against business rules to find any forms in error. IRIS then packages the submission, to only contain those forms in error, and sends it to IRRP to be redressed. IRRP will receive these submissions from the Redress API and will return redressed data to the Redressed API. In order to persist and redress data throughout the portal, IRRP will store data received from the Redress API in a local database until it is returned to IRIS with updates made. The application resides on AWS GovCloud, CSP Package ID: F1603047866 Within the application, Managers, Tax Examiners, and Quality Reviewers perform different roles. Managers are able to view all inbound Information Returns, assign Information Returns to Tax Examiners for redress, assign redressed Information Returns to Quality Reviewers for review, and submit completed IRs back to IRIS. Tax Examiners view the fields in error for each IR and then make the necessary updates. Quality Reviewers receive already redressed IRs and can review and make additional updates. All roles can flag forms for fraud or deletion.

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:

Interfaces with external entities that require the SSN

Delivery of governmental benefits, privileges, and services

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

The Employee Portal require the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal

Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. Customer service and paper submission process usage.

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 Cir. 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.

Employer Identification Number

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)
Medical Information
Vehicle Identifiers
Employment Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

No

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

No

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

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 Employee Portal (IRRP) is used for Tax Administration purposes. The Information Returns Review Portal (IRRP) is a digital portal being developed to replace in-person Submission Processing and the legacy Error Resolution System (ERS). IRRP will be used by IRS Employees who can use this portal to complete the redress process for submissions found with forms in error. The process begins with SCRIPS, a paper-form digitization service, which sends digitized submissions to IRIS. IRIS then validates the form data against business rules to find any forms in error. IRIS then packages the submission, to only contain those forms in error, and sends it to IRRP to be redressed. IRRP will receive these submissions from the Redress API and will return redressed data to the Redressed API. In order to persist and redress data throughout the portal, IRRP will store data received from the Redress API in a local database until it is returned to IRIS with updates made. The Employee Portal will be used in conjunction with the IRIS Web Portal to assist customers with transmitter support. The Employee Portal will allow IRS employees to view SBU/PII information collected from the IRIS Web Portal.

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

It is the responsibility of the business trading partner who sends the data to ensure it is correct, timely, and complete. The Employee Portal leverages Information Return Intake Service (IRIS) for validation and completeness.

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 24.046	Customer Account Data Engine Business Master File
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 22.062	Electronic Filing 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: Active Directory Federation Services (ADFS) Single Sign-On (SSO)
Current PCLIA: No
SA&A: No

System Name: Submission Processing and the legacy Error Resolution System (ERS)
Current PCLIA: No
SA&A: No

System Name: Negative TIN Check (NTIN)
Current PCLIA: No
SA&A: No

System Name: Information Return Intake Service (IRIS)
Current PCLIA: Yes
Approval Date: 5/20/2022
SA&A: No

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?

Yes

Please identify the form number and name:

Form Number: 1099
Form Name: MISC

Form Number: 1099
Form Name: NEC

Form Number: 1099
Form Name: H

Form Number: 1099
Form Name: INT

Form Number: 1099
Form Name: S

Form Number: 1099
Form Name: DIV

Form Number: 1099
Form Name: R

Form Number: 1099
Form Name: B

Form Number: 1099
Form Name: PATR

Form Number: 1099
Form Name: C

Form Number: 1099
Form Name: G

Form Number: 1099
Form Name: K

Form Number: 1099
Form Name: A

Form Number: 1099
Form Name: OID

Form Number: 1099
Form Name: CAP

Form Number: 1099
Form Name: LTC

Form Number: 1099
Form Name: Q

Form Number: 1099
Form Name: SA

Form Number: 1099
Form Name: LS

Form Number: 1099
Form Name: QA

Form Number: 1099
Form Name: SB

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Information Return Intake Service (IRIS)
Current PCLIA: Yes
Approval Date: 5/20/2022
SA&A: No

System Name: Submission Processing and the legacy Error Resolution System (ERS)
Current PCLIA: Yes
Approval Date: 7/23/2022
SA&A: No

Identify the authority.

Taxpayer First Act's Section 2102 Mandate

For what purpose?

For tax administration purposes

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

6/21/2016

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

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?

All forms come with instructions on what is required. The information within the Employee Portal comes from the IRIS Web Portal and includes various forms. This system and forms provide the Privacy Act Notice to individuals. The Employee Portal do not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent, and due process are provided via the IRS system and their related tax forms instructions, and pursuant to 5 USC.

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

No

Why not?

The users are internal IRS employees that are going through IRS system access request, to obtain authority to view/correct production data. Consenting to use of information is automatically validated through the authentication and authorization process.

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

After checking status to find out that their submission contains an error or was rejected, the submitter can correct the error(s) in their own environment and re-submit. The rejection response from the IRS to the submitter will include details as to why the submission was rejected. Likewise, in the case of incorrect information that does not cause a reject, the submitter will be informed as to exactly what elements are incorrect. Transmitters will have access to IRS personnel (dedicated phone lines), as well as documentation (published documents as well as material at IRS.gov) to assist them in interpreting the responses, making necessary corrections, and resubmitting the transmission.

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 Write

Managers: Read Write

System Administrators: Read Write

Developers: Administrator

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Write

Contractor Developers: Read Write

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

Access to Employee Portal is determined by the role of the employee and maintained through BEARS (Business Entitlement Access Request System) formerly known as OL5081 (system access request), which is approved by managers and system administrators. Access is based on hierarchy roles and permissions.

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.

All records housed in the Employee Portal will be erased or purged from the system in accordance with approved retention periods. IRS Web Portal data retention is done in accordance with RCS item 29 and items 85, 87, 88, and 129 in addition to IRM 1.15.6 Managing Electronic Records. All records will be destroyed in accordance with the applicable Records Control Schedules. Audit Records are retained in accordance with GRS 3.2, item 030 and 031.

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?

1/3/2022

Describe the system's audit trail.

The system will be using Integrated Enterprise Portal (IEP) audit trail. The IEP audit trail capability is documented in detail in the IRIS Web Portal/Employee Portal System Security Plan. This document and related security documents which contain IEP audit information are regularly updated and reviewed. Integrated Enterprise Portal (IEP) systems are connected to a centralized log management solution. Auditable events are transmitted via secured connections for real-time analysis of security alerts generated by network devices, hardware, and applications. Logs and alerts are analyzed, correlated, classified, and interpreted by security analysts. The collection and management of auditable data compiles with IRS, Treasury and other federal requirements which require the following data elements to be audited.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

No

When is the test plan scheduled for completion?

8/9/2023

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?

Stored in internal team SharePoint site.

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: 50,000 to 100,000
Contractors: Not Applicable
Members of the Public: More than 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