Date of Approval: 07/01/2025
Questionnaire Number: 2084

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

Employee Portal (Information Returns Review Portal)

Acronym:

IRRP

Business Unit

IT - Cybersecurity

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Sponsor

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

Information Returns Review Portal (IRRP) application is used by IRS Employees, who logs 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 Service Center Recognition/Image Processing System (SCRIPS), a paper-form digitization service, which sends digitized submissions to Information Return Intake System (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 Application Programming Interface (API). IRRP stores data received from the Redress API in a local database until it is returned to IRIS with updates made. Within the

application, Managers, Tax Examiners, and Quality Reviewers perform different roles. Managers can 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 Information Returns (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.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?
　　　Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).
　　　Data: Information Returns Review Portal (IRRP) only uses sensitive data to identify and resolve problematic records or if defects are found in our code. Any data used in this will have sensitive data removed or masked. We also allow the business to pull quantitative metrics that has sensitive data removed. Creation: Sensitive data such as Taxpayer Identification Number (TIN), Employer Identification Number (EIN) and Social Security Number (SSN), addresses, telephone numbers, etc. are required and included when a user corrects a form within the IRRP application. Storage Once the user "saves" the form, the data is stored as a document (record) in MongoDB database collection. Direct access to this database is controlled by authentication and monitored. Only people with business use reasons are given access. The application uses a service account to access the database. The Cloud Team and DBAs manage the service accounts used by the applications. Use: IRRP is intended to allow IRS employees to view forms and submit corrections. The initial data is retrieved from the IRIS Application Programming Interface (APIs). During the correction process the form data is stored in MongoDB. MongoDB has the same systems in place to prevent unauthorized access of data. Sharing: Data is shared with the IRIS system through the submission process, which securely transmits a copy of the selected form data in the Taxpayer Portal MongoDB to IRIS APIs for processing and storage on their end. Archiving: Unclassified data is retained for 7 years which is based on the "IRS General Records Schedule."

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.
　　　Address
　　　Email Address
　　　Employer Identification Number

Employment Information
Federal Tax Information (FTI)
Financial Account Number
Internet Protocol Address (IP Address)
Medical History/Information
Name
Other
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Telephone Numbers
Vehicle Identification Number (VIN)

Please explain the other type(s) of PII that this project uses.
Date of Birth

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for personnel administration IRS employees - 5 USC and Executive Order 9397
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?
No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?
Application

3 What Tier designation has been applied to your system?
0

4 Is this a new system?
No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?
Yes

4.11 What is the previous PCLIA number?
8264

4.12 What is the previous PCLIA title (system name)?
    Employee Portal (Information Returns Review), IRRP

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)
    The Privacy auditor from the Cloud Annual Security Control Assessment (C-ASCA) team required the system to update Q. 26 of the privacy form to provide justification of using TINs in the audit logs.

5 Is this system considered a child system/application to another (parent) system?
    No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.
    Execution

7 Is this a change resulting from the OneSDLC process?
    No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.
    Web Applications Governance Board; reporting to Strategic Development Executive Steering Committee ESC committee (SD-ESC)

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.
    211833

10 If this system discloses any PII to any third party outside the IRS, does the system have a process in place to account for such disclosures in compliance with IRC 6103(p)(3)(A) or Subsection c of the Privacy Act?
    Yes

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?
    No

12 Does this system use cloud computing?
    Yes

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

      Integrated Enterprise Portal (IEP), (F1603047866), 06/21/2016

12.2 Does the CSP allow auditing?

      Yes

12.21 Who has access to the CSP audit data (IRS or 3rd party)?

      IRS

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

      Moderate

13 Does this system/application interact with the public?

      No

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

      After checking status to find out that their submission contains an error or was rejected, the submitter can correct the error(s) in his/her own environment and re-submit. The rejection response from the IRS to the submitter will include details as to why the submission was rejected. 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.

15 Is this system owned and/or operated by a contractor?

      Yes. IRS Owned and Contractor Operated

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

      IRS Employees - Access Level
      Users - Read and Write
      Managers - Read and Write
      Sys. Administrators - Read and Write
      Developers - Administrator
      Contractor Employees - Yes/No - Access Level - Background Invest. Level
      Contractor Users - Yes - Read and Write - Moderate
      Contractor Managers - Yes - Read and Write - Moderate
      Contractor Sys. Administrators - No
      Contractor Developers - Yes - Read and Write - Moderate

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

Thank you for visiting the Internal Revenue Service's website, an official United States Government System, and reviewing our privacy policy. Our privacy policy explains how we handle the personally identifiable information (PII) that you provide to us when you visit us online to browse, obtain information, or conduct a transaction. PII includes information that is personal in nature, and which might be used to identify you. The IRS uses this website to provide information about IRS services and programs. This website includes specific applications which provide more services or enable us to respond to specific questions from website visitors. We won't collect personal information about you just because you visit this Internet site. Some applications on this website provide you with the opportunity to order forms, ask questions requiring a response, sign up for electronic newsletters, participate in focus groups and customer surveys, or learn the status of filed returns or anticipated payments. Using these services is voluntary and may require that you provide additional personal information to us. Providing the requested information implies your consent for us to use this data to respond to your specific request. All personal information you provide to us is voluntary. We may collect personal information about you (such as name, email address, Social Security number or another unique identifier) only if you specifically and knowingly provide it to us. We will use your information to process requests for certain services or information. Providing your information is generally voluntary, but if it is not provided, we might not be able to process your transaction. When information is required, we will let you know before we collect it. We publish specific information on records the IRS may collect in the IRS Privacy Act System of Records Notices on the U.S. Department of the Treasury System of Records Notices page. We collect PII and other information only as necessary to administer our programs under the authority of the Internal Revenue Code and the protections of the Code and the Privacy Act. The information you provide will be used only for that purpose. We do not sell the information collected at this site or any other information we collect. You do not have to give us personal information to visit our website. For more information on authority, visit the agency, its mission and statutory authority page. We publish specific information on the purpose and authority for records the IRS may collect in the IRS Privacy Act System of Records Notices on the U.S. Department of the Treasury System of Records Notices page. Throughout our website, we will let you know if the information we ask you to provide is voluntary or required. By providing your personal information, you give us consent to use the information only for the purpose for which it was collected. We describe those purposes when we collect information. We will ask for your consent before using the information you provide for any secondary purpose other than those required by federal law. We will disclose your information only authorized by law and as listed in the

routine uses published in the IRS Privacy Act System of Records Notices on the U.S. Department of the Treasury System of Records Notices page. We protect your information in a secure and readily accessible environment. We also monitor network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage to the web service. We focus on web site security so that this service remains available to you and other visitors. No attempts are made to identify individual users unless illegal behavior is suspected. For more information on security, visit our security of your information page.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".
    Not Applicable

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".
    Not Applicable

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".
    100,000 - 1,000,000

22 How is access to SBU/PII determined and by whom?
    Access to Employee Portal is determined by the roles of the employees and maintained through BEARS (Business Entitlement Access Request System) and must be approved by managers and system administrators. Access is based on hierarchy roles and permissions.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.
    No

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.
    Yes

26 Describe this system's audit trail in detail. Provide supporting documents.
    The system is using Integrated Enterprise Portal (IEP) and Enterprise Security Audit Trails (ESAT) Audit trails. These audit trail capabilities are documented in the Information Return Intake System (IRIS) Web Portal Audit Worksheet as follows: - Auditable events are transmitted via secured connections for real-time analysis of security alerts generated by network devices, hardware and applications. - TINs are included in the audit logs to identify user's access; necessary for Unauthorized Access of Taxpayer Records (UNAX) correlation as part of the UNAX program and assisting with Treasury Inspector General for Tax Administration (TIGTA) Office of Investigation with UNAX detection and

investigations. - Logs and alerts are analyzed and send to system administrator and Information Systems Security Officer (ISSO).

27 Does this system use or plan to use SBU data in a non-production environment?
No

Interfaces

Interface Type
IRS Systems, file, or database
Agency Name
Information Returns Intake System (IRIS)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Integrated Enterprise Portal (IEP)
Other Transfer Method
Information is sent from IRIS to IRRP via API calls.

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
General Support System (GSS)-Integrated Enterprise Portal (IEP) processes electronic records on-behalf of hosted applications, audit trails associated with this processing are sent to IRS Enterprise Security Audit Trails (ESAT) for central log aggregation.

SORN Number & Name
IRS 24.030 - Customer Account Data Engine Individual Master File
Describe the IRS use and relevance of this SORN.
To maintain records of tax returns, return transactions, and authorized taxpayer representatives.

SORN Number & Name
IRS 22.062 - Electronic Filing Records
Describe the IRS use and relevance of this SORN.
Underlying storage components within General Support System (GSS)-IEP may be used to store or process Electronic Filing Records on behalf of hosted applications.

Records Retention

What is the Record Schedule System?
>	General Record Schedule (GRS)

What is the retention series title?
>	System Access Records

What is the GRS/RCS Item Number?
>	GRS 3.2 item 31

What type of Records is this for?
>	Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.
>	These records are created as part of the user identification and authorization process to gain access to systems.

What is the disposition schedule?
>	Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

What is the Record Schedule System?
>	Record Control Schedule (RCS)

What is the retention series title?
>	Taxpayer Services

What is the GRS/RCS Item Number?
>	RCS 29 items 85

What type of Records is this for?
>	Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.
>	Information Returns and related documents submitted by domestic and foreign firms to advise the names, amounts and types of income paid to individuals.

What is the disposition schedule?
>	All records will be destroyed in accordance with the applicable Records Control Schedules disposition.

What is the Record Schedule System?
>	Record Control Schedule (RCS)

What is the retention series title?
>	Taxpayer Services

What is the GRS/RCS Item Number?
>	RCS-29 item 87

What type of Records is this for?
>	Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.
>	Undelivered Information Returns (Copy B).

What is the disposition schedule?

Returns transmitted by employers, payers and nominees to the service center (Foreign W-2). Disposition: AUTHORIZED DISPOSITION Destroy January 2 following the year in which prepared. (2) All Forms 1099 issued by Treasury, if research indicates no new address and no DLN is located to associate with the form. AUTHORIZED DISPOSITION Destroy upon receipt

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Taxpayer Services

What is the GRS/RCS Item Number?

RCS-29 item 88

What type of Records is this for?

Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.

Information Returns received from employees and recipients (Foreign W-2).

What is the disposition schedule?

(1) Information Returns associated with income tax returns. AUTHORIZED DISPOSITION Destroy or Retain, as appropriate, when related income tax returns are destroyed or retired. (2) Information Returns not associated with related income tax returns. AUTHORIZED DISPOSITION Destroy January 2 following the year in which prepared.

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Taxpayer Services

What is the GRS/RCS Item Number?

RCS-29 item 129

What type of Records is this for?

Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.

Statement for Recipients of Interest Income (Form 1099-INT Copy C). Issued by the Service Center for interest payment in excess of $10.00.

What is the disposition schedule?

AUTHORIZED DISPOSITION Destroy 6 years and 3 months after the calendar year issued.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?
> System Access Records

What is the GRS/RCS Item Number?
> GRS 3.2 item 30

What type of Records is this for?
> Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.
> These records are created as part of the user identification and authorization process to gain access to systems.

What is the disposition schedule?
> Destroy when business use ceases.

Data Locations

What type of site is this?
> System

What is the name of the System?
> Information Returns Database (IRDB)

What is the sensitivity of the System?
> Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.
> IRDB will be the authoritative information returns database component of the IR Mod Program. IRDB supports Information Returns Processing System (IRPS) Data Certification (Deduplication, Payer Fraud Marking, ALE Identification, Completeness, Corrected Returns, and Deceased Marking) and sends data to downstream systems.

What are the incoming connections to this System?
> 1. Information Return Intake System Database (IRIS DB) - Stores information Return (IR) 2. As-Received contains Information received without modification from User or System 3. IRPS contains IR Data Certification and Data Quality/Validation Services. The IRPS validates, reconciles, and certifies IR data in the IRDB for further processing by downstream systems.