

Date of Approval: 11/04/2025
Questionnaire Number: 2469

Basic Information/Executive Summary

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

Information Returns Processing System

Acronym:

IRPS

Business Unit

Taxpayer Services

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.

The general purpose of the Internal Revenue Service (IRS) Information Return Processing System (IRPS) is to support the processing of information returns to improve data quality and provide data for assisting downstream compliance systems to identify fraud. IRPS supports the following enterprise and core services:

- Enterprise Services

1. As-Received (AsR): AsR supports the storage and lookup of documents as they are received and accepted by the IRS before any other processing is done.
2. Information Return Data Access Service (IRDAS): IRDAS is a common Application Programming Interface (API) for access to all Information Returns (IR) Data for up to 10 tax years.

3. Identity Data Quality (IDQ): IDQ services support Taxpayer Identification Number (TIN) Validation and TIN Perfection, ultimately increasing data consistency.

- Core Services

1. Information Data Integration (IDI): IDI supports downstream systems for Civil Penalty processing and other compliance activities.

2. Information Data Certification (IDC): IDC services are designed to improve the Affordable Care Act (ACA) and Partnership Bipartisan Budget Act (PBBA) data quality and provide metadata for use by downstream compliance processes.

3. Information Data Reconciliation (IDR): IDR services are designed to treat ACA information returns containing contradictions, errors, and missing data, and translate into a consistent, valid representation to improve the data quality for post-filing compliance activities and data analytics.

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).

Within the Information Returns (IR) lifecycle, sensitive data such as personally identifiable information (PII), Social Security Numbers (SSNs), Employer Identification Numbers (EINs), Individual Taxpayer Identification Numbers (ITINs), Preparer Tax Identification Numbers (PTINs), and Document Locator Numbers (DLNs), is handled in accordance with defined agency business unit needs and federal records management standards. At the As Received (AR) stage, identifiers are captured in their raw form from both paper and electronic filings and logged for routing and audit purposes. During Information Data Integration (IDI), identifiers are parsed and associated with their corresponding return records, linking taxpayer information to form types, submission sources, and initial processing controls. During Information Data Certification (IDC), SSNs, EINs, and ITINs are verified against IRS Master Files; PTINs are validated against the CAF/preparer registry; and DLNs are confirmed for batch integrity. Within Information Data Reconciliation (IDR), identifiers are leveraged to detect duplicates, correct common errors, and ensure consistency across forms while maintaining submission traceability. During IDR, identifiers serve as the keys for aligning taxpayer accounts, generating compliance reports, and enforcing preparer oversight. DLNs maintain the end-to-end audit trail across all processing stages. Disposition: IRPS does not destroy or delete PII after use. All identifiers are retained in compliance with IRS Privacy, Governmental Liaison, and Disclosure (PGLD) guidance and the National Archives and Records Administration

(NARA) retention schedules. Records are archived securely and preserved for the legally mandated retention and retrieval period to support oversight, enforcement, and discovery.

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

Address
Employer Identification Number
Employment Information
Federal Tax Information (FTI)
Internet Protocol Address (IP Address)
Name
Other
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number

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 tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

No

1.1 What is the name of the Business Unit (BU) or Agency initiative?

Wage & Investment / Small Business Self Employed

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

System

3 What Tier designation has been applied to your system? (Number)

4

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?

1344

4.12 What is the previous PCLIA title (system name)?

Information Returns Processing System (IRPS)

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.)

Changes to PII (Inclusion of IP addresses).

5 Is this system considered a child system/application to another (parent) system?

Yes

5.1 Identify the parent system's approved PCLIA number.

7460

5.2 Identify the parent system's name as previously approved.

Information Returns Processing (IRP)

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.

Corporate Data Governance Board

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.

210636

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?

No

10.1 You have indicated that you do not have an "accounting of disclosures" process in place; please indicate a projected completion date or explain the steps taken to develop your accounting of disclosures process. Note: The Office of Disclosure should be contacted to develop this system's accounting of disclosures process.

No

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.

Cloud Service Provider (CSP): Amazon Web Services (AWS) GovCloud

FedRAMP Package ID F1603047866 Date Authorized - 06/21/2016

12.2 Does the CSP allow auditing?

Yes

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

None

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)

IRPS is a backend system and therefore not accessible to the public. In the event an individual would need to access or correct their information, the individual would do so by accessing an upstream/externally facing system and/or submitting the appropriate corrected tax form(s) to the IRS.

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

Yes

15.1 If a contractor owns or operates the system, does the contractor use subcontractors; or do you require multiple contractors to operate, test, and/or maintain this system?

Yes

15.2 What PII/SBU data does the subcontractor(s) have access to?

Date of Birth, Address, Employer Identification Number, Employment Information, Federal Tax Information (FTI), Internet Protocol Address (IP Address), Name, Other, Social Security Number (including masked or last four digits), Standard Employee Identifier (SEID), Tax ID Number.

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.)

For all who have access to IRPS, a Moderate Background Investigation (MBI) is conducted and an SBU waiver submitted for access to PII data for both IRS employees and contractors. IRPS utilizes the IRS Business Entitlement Access Request System (BEARS) to facilitate and document access approval. Data access is granted on a need-to-know basis. A potential user must submit a request for access via BEARS to management for approval consideration. Specific permissions are defined on the BEARS form and set (activated) by the System Administrator prior to the user being allowed access. Management monitors system access and removes permissions when individuals no longer require access. IRS Employees: User - (Read Only) Manager - (Read and Write) Developer - (Read and Write) IRS Contractors: User - (Read Only) Developer - (Read and Write)

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.

IRPS does not interact with the public, but rather the information returns completed by taxpayers contain Privacy Act Statements

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".
More than 1,000,000.

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

The IRPS system utilizes the IRS On-Line application BEARS application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access via IRS BEARS to their local management for approval consideration. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the BEARS form and set (activated) by the System Administrator prior to the user being allowed access. Management monitors system access and removes permissions when individuals no longer require access.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

Yes

24 Explain any privacy and civil liberties risks related to privacy controls.

IRPS is an internal system. This architectural boundary, combined with role-based access controls, audit logging, encryption, and network segmentation, ensures that identifiers are protected from unauthorized access. Where feasible, identifiers are redacted or masked in reports and external outputs. These layered measures ensure that SSNs, EINs, ITINs, PTINs, and DLNs are not disposable elements but business-critical identifiers whose use is restricted to defined, auditable purposes and retained in full compliance with federal privacy and records management requirements.

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.

No

26 Describe this system's audit trail in detail. Provide supporting documents.

Audit trails are captured through integrated Splunk logging mechanisms and native system-level logs, ensuring comprehensive traceability across application and infrastructure components.

27 Does this system use or plan to use SBU data in a non-production environment?

Yes

27.1 Please upload the Approved Email and one of the following SBU Data Use Forms, Questionnaire (F14664) or Request (F14665) or the approved Recertification (F14659). Select Yes to indicate that you will upload the Approval email and one of the SBU Data Use forms.

Yes

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

Information Returns Processing Incorrect Information Penalty
(IRPIIP)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Digitalization and Scanning as a Service (DIGSCaaS)

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Payer Master File (PMF)

Incoming/Outgoing

Both

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Information Returns Master File Processing (IRMF)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

Enterprise Service Bus (ESB)

Incoming/Outgoing
Both
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
ISR Sharing (ISRS)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Secure Access Digital Identity (SADI)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Clean Energy (CE)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Backup Withholding (BWH)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Information Returns Processing Input Processing (IRPIP)

Incoming/Outgoing
Both
Transfer Method
Application to Application (A2A)

Interface Type

IRS Systems, file, or database
Agency Name
Information Returns Intake System (IRIS)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

Interface Type

IRS Systems, file, or database
Agency Name
Information Returns Database (IRDB)
Incoming/Outgoing
Both
Transfer Method
Application to Application (A2A)

Interface Type

IRS Systems, file, or database
Agency Name
Correspondence Examination Automation Support (CEAS)
Incoming/Outgoing
Both
Transfer Method
Application to Application (A2A)

Interface Type

IRS Systems, file, or database
Agency Name
Enterprise Informatica Platform (EIP)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Application to Application (A2A)

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.

IRPS receives, validates, and certifies IR data for further processing by downstream systems. IRPS services include AsR, IDI, IDQ, IDC, and IDR.

SORN Number & Name

IRS 22.062 - Electronic Filing Records

Describe the IRS use and relevance of this SORN.

IRPS receives, validates, and certifies IR data for further processing by downstream systems. IRPS services include AsR, IDI, IDQ, IDC, and IDR.

SORN Number & Name

IRS 22.061 - Information Return Master File

Describe the IRS use and relevance of this SORN.

IRPS receives, validates, and certifies IR data for further processing by downstream systems. IRPS services include AsR, IDI, IDQ, IDC, and IDR.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

RCS 22/Affordable Care Act (ACA) Information Returns Database (IRDB)

What is the GRS/RCS Item Number?

56

What type of Records is this for?

Both (Paper and Electronic)

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

Affordable Care Act (ACA) Information Returns Database (IRDB). IRDB receives and stores validated electronic Form 1095-A (Health Insurance Marketplace Statement), Form 1094-B (Transmittal of Health Insurance Coverage Statements), Form 1094-C (Transmittal of Employer-Provided Health Insurance Offer and Coverage Information Returns), Form 1095-B (Health Insurance Coverage) and Form 1095-C (Employer-Provided Health Coverage) ACA Information Return Data to support ACA

and Current Production Environment (CPE) Processes, as well as Fact of Filing data from paper F 1094 series returns. There is no IRDB interface for viewing or altering the records stored in any IRDB schemas. All data contained in IRDB is maintained in its original state, with no change to the integrity or quality of the data. IRDB does not manipulate or apply business rules to the data. (Job No. DAA-0058-2016-0019-0001)

What is the disposition schedule?

Cut off data at the end of the calendar year. Delete/Destroy data 3 years after cutoff.

Data Locations

What type of site is this?

System

What is the name of the System?

Splunk

What is the sensitivity of the System?

Federal Tax Information (FTI)

Please provide a brief description of the System.

Splunk is currently utilized by IRPS as a data monitoring, tagging, and storage information.

What are the incoming connections to this System?

Upstream Interfaces noted in the locations section.

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

What is the URL of the item, if applicable?

http://ea.web.irs.gov/aba/index.html?mainpageurl=SA/ea-panel1_main-application_7518.htm

Please provide a brief description of the System.

The general purpose of Information Return Processing System (IRPS) is to support processing of information returns to improve data quality and provide data for assisting downstream compliance systems to identify fraud and assess incorrect information penalties. IRPS supports four capabilities which are: Identity Data Quality (IDQ): IDQ consists of identity a Taxpayer Identification Number (TIN+Name Control) validation micro services and batch processes for identity data validation and perfection Taxpayer Identification Number (TIN+Name Control) found from Name and

Address search). IR Data Certification (IDC): IDC services are designed to improve the Affordable Care Act (ACA) and Partnership Bipartisan Budget Act (PBBA) data quality and provide metadata (information about the data) for use by downstream compliance processes. IR Data Reconciliation (IDR): IDR services are designed to treat Affordable Care Act (ACA) Information Returns containing contradictions/errors/missing data and translate into a consistent, valid representation to improve the data quality for Post-Filing Compliance activities and Data Analytics, and IR Data Integration (IDI) supports downstream systems for Civil Penalty processing and other compliance activities.

What are the incoming connections to this System?

IRMF/PMF - IRPS receives PII information from upstream systems/IRDB as a message request and digested for validation by application like TINV services and also receive reference files from legacy system/mainframe for tin validation and fraud purposes, which contain TIN information disseminated to downstream IRS systems. This impacts the Discovery by Address Validation, Discovery by Date of Birth, Recipient Tin Validation, Issuer Tin Validation, Discovery by Address Controller, Supplemental Controller, UVC Controllers, and Reference Data Converter Controller services.

What are the outgoing connections from this System?

IRDB/CEAS Databases - Data is disseminated to these databases for downstream IRS systems to access for our IDC, IDQ, IDI and IDR services. ESB - For services such as PBBA IDC Refactor, data is disseminated from ESB to IRPS and eventually downstream systems. This data includes 8985/8986 forms sent to us to perform our logic.