Date of Approval: 06/05/2026
Questionnaire Number: 3045

Basic Information/Executive Summary

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

Taxpayer Services Identity Personal Identification Number (IP PIN) Reissuance

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 Taxpayer Services Identity Protection Personal Identification Number (IP PIN) Reissuance automation is a Robotic Process Automation (RPA) project owned by Taxpayer Services and operated by authorized Taxpayer Services employees who process IP PIN reissuance requests. The automation is developed and maintained by the Internal Revenue Service (IRS) RPA team. This project automates the process used to reissue IP PINs to taxpayers. Currently, employees must manually retrieve requests, validate taxpayer information, perform research, process reissuance actions, generate correspondence, and record results in IRS systems. These activities are repetitive, time-consuming, and can occupy employee workstations for extended periods. The automation receives reissuance requests from a processing queue, loads the information into secure database tables, validates taxpayer information, and processes the reissuance through the Integrated Data Retrieval System (IDRS) and Generalized Integrated IDRS Keying and Research Access Database (GIIKRAD). The automation generates the required taxpayer correspondence, records processing results, and identifies any

exceptions requiring employee review. By automating these routine tasks, the project reduces manual effort, improves processing accuracy, decreases workstation utilization, and enables employees to focus on higher-value taxpayer service activities. This supports the IRS mission by improving operational efficiency, strengthening identity protection, and providing faster and more consistent service to taxpayers.

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).

This project processes sensitive taxpayer data, including Taxpayer Identification Numbers (TINs), names, addresses, and Identity Personal Identification Numbers (IP PINs), to support the reissuance process. Data is received from authorized IRS sources as queued requests and is limited to the minimum necessary elements. The RPA securely ingests the data and stores it in designated SQL database tables for processing. It uses data to validate taxpayer identity, generate GIIKRAD files, interact with IDRS, reissue IP PINs, and produce correspondence such as Letter 4869C. All processing occurs within IRS-controlled environments, with data encrypted in transit and at rest and access restricted through role-based controls. Data is only shared internally between authorized IRS systems, including SQL databases and IDRS, with no external dissemination. Records are retained in accordance with IRS records schedules for only as long as necessary. Temporary processing data and intermediate files are deleted after use, and all data is disposed of following IRS-approved sanitization and destruction standards.

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

Address
Document Locator Number (DLN)
Family Members
Federal Tax Information (FTI)
Name
Other
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)

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

Taxpayer Identification Numbers (TINs), Identity Personal Identification Number (IP PINs)

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

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
PII for personnel administration - 5 USC
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

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

Yes

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

Robotic Process Automation

2 Describe in detail, the Robotic Process Automation (RPA) process; be sure to identify the project title and business unit owner; state what IRS Strategy or initiative it supports; identify the system or process it supports and if PII will be required for the RPA to run; identify activities and workflow controls with the type and capabilities that will be incorporated; lastly indicate how the service benefits from the use of this RPA. (Process, Library, Test Automation, Template.)

This RPA supports IRS modernization and taxpayer service initiatives by improving efficiency, accuracy, and identify protection. It automates the IP PIN reissuance process, which is currently manual and resource intensive. The automation retrieves queued taxpayer requests, loads data into secure Secured Query Language (SQL) tables, and executes an application to validate IP PIN data. It generates GIIKRAD files to interact with IDRS, uses command codes to reissue IP PINs, produces correspondence (Letter 4869C), and records results back into the system. The process requires PII, including TINs, names, addresses, and IP PIN data, to validate identity and process requests. Workflow controls include input validation, rule-based processing, exception handling, and audit logging, with role-based access and least-privilege principles enforced. This solution is implemented as a process automation using reusable libraries, templates, and structured testing. The RPA reduces manual workload and errors, prevents workstation disruption, and accelerates processing, resulting in improved taxpayer service and stronger identity protection.

3 Is this a new Robotic Process Automation (RPA) project?

Yes

4 Identify the IRS IT systems, applications, projects, and/or databases this RPA is applied to; include the associated system name.

Taxpayer Services Identity Personal Identification Number (IP PIN) Reissuance automation applies to the following systems:

- IDRS is used to verify taxpayer entity information and confirm accuracy of records during validation and creation processes.
- Generalized Integrated IDRS Keying and Research Access Database (GIIKRAD) provides users with a structured interface to input, research, and manage taxpayer account data within IDRS.
- Taxpayer Services Database is where taxpayer entity records are queried, validated, updated, and stored.
- Taxpayer Assistance Center (TAC) Input Queue/System provides incoming TIN records and associated taxpayer data for processing by the RPA.

5 Identify why the use of SBU/PII/FTI is required; include any type of Sensitive But Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI) that this project will create, collect, receive, use, process, maintain, access, inspect, display, store, disclose, disseminate, or dispose of.

The taxpayer's PII, SBU Data and FTI which includes their SSN, name, address, and tax return information is used to retrieve and verify information required for processing their request for the reissuance of their IP PIN.

6 Is your RPA Attended/Unattended?

Attended

7 Is this RPA process converting from paper to electronic format or automating a process currently performed by a human?

Yes

7.1 Explain the process being replaced/automated.

The RPA replaces a manual process used to reissue Identity Protection Personal Identification Numbers (IP PINs). Currently, IRS personnel retrieve queued requests, manually generate and input data into SQL tables, and access IDRS through GIIKRAD to validate taxpayer information. Employees use command codes to process reissuance, generate required correspondence (Letter 4869C), and verify results. This process is time-consuming, repetitive, and can occupy employee workstations, limiting productivity. It also requires repeated handling when errors or incomplete data occur. The RPA automates these steps by retrieving queued requests, generating and processing SQL data, interacting with IDRS through GIIKRAD, executing command codes, and recording results. Exception cases are routed to employees for review, ensuring oversight while reducing manual effort and improving efficiency.

8 Indicate what level of complexity the RPA is classified as and if you were required to register with One Solution Delivery Lifecycle (OneSDLC) or not, or indicate if Information Technology's (ITs) Technical Insertion process was used for approval of this RPA.

This RPA is classified as a moderate complexity automation. While it is primarily rules-based, it involves integration with multiple IRS systems (including the Taxpayer Services Database and IDRS), processing of sensitive data (PII/FTI), and implementation of validation, exception handling, and audit controls. These factors increase its complexity beyond basic task automation.

9 Will connections or interdependencies be established for this RPA?

Yes

9.1 Will the connection be encrypted?

Yes

9.2 Will authentication/credentials be required?

Yes

9.3 Please provide details for the connection/interdependency. Indicate if this occurs on the backend versus through the system/user interface.

Interdependencies exist between systems, as data is processed sequentially from the input queue to validation, update, or creation, with IDRS used for verification. Limited backend components (e.g., executables or scripts) support queue management and processing; however, core system interactions--especially with IDRS--occur through the user interface. All connections occur within the IRS network using secure authentication, ensuring data remains within authorized environments and is handled in compliance with security and audit requirements. The connections are also through the ECLAS API, which will connect via the backend.

10 Indicate who has or will have permission to access the data and how users are authenticated.

Access to the data is restricted to authorized IRS personnel, approved system administrators, and the RPA service account responsible for executing the automation. Access is granted based on role-based access controls (RBAC) and least-privilege principles to ensure users only have access necessary to perform their job functions. Users are authenticated through existing IRS network authentication and access management controls, including secure login credentials. The RPA uses dedicated service credentials to securely access authorized systems and applications. All access and system activities are logged and monitored for auditing and compliance purposes.

11 Indicate if Business Entitlement Access Request System (BEARS) entitlements are required for access and if Privileged User Management Access System (PUMAS) control management is applied for granting access to the system(s)? If BEARS/PUMAS are not applied, indicate what access controls are in place.

BEARS entitlements will be required to request and approve access to InfoConnect, GIIKRAD, IDRS, and Account Management Service (AMS). Access will be granted based on business need and role-based access control principles. Data access is granted on a need-to-know basis. BEARS enrollment process requires that an authorized manager approve access requests on a case-by-case basis. Users are given the minimum set of privileges required to perform their regular and recurring work assignments; they are restricted from changing the boundaries of their access without management approval. Write, Modify, Delete, and/or Print are defined on BEARS and set (activated) by the System Administrator prior to user being allowed access. User privileges and user roles determine the types of data that each user has access to management monitors system access and removes permission when individuals no longer require access.

12 Identify the maintenance tasks or updates performed; state whether or not the maintenance tasks are inherited from the host (UiPath Platform) or you are using customized maintenance activities.

UiPath will use Security Assertion Markup Language (SAML) for UiPath Orchestrator.

13 Indicate if this product or system shares data outside of the United States or its territories.

No

14 Indicate if this system or Robotic Process Automation (RPA) is trained through the use of algorithms; indicate if the algorithm used contains data with a sensitivity classification. (Sensitive but unclassified data might include algorithms, methods, system data, or PII/FTI that could be used to re-identify a person.)

The RPA utilizes algorithms to perform automated processing and decision-making functions. The algorithms may process, store, or interact with Sensitive But Unclassified (SBU) data, including potentially Personally Identifiable Information (PII), Federal Tax Information (FTI), system data, business rules, methods, or other information that could be used to identify or reidentify an individual. Appropriate security and privacy controls are implemented to protect sensitive data in accordance with applicable federal and organizational requirements.

15 Describe this system's (RPAs) audit trail process in detail; include location of supporting documents (SPLUNK). Note: Upload of this document is required.

The RPA system's trail process is crucial for maintaining transparency and accountability, generating detailed logs of all bot actions, including timestamps, data manipulations, and user interactions. These logs are then stored in a

centralized repository, ensuring data integrity and restricted access. Splunk plays a vital role in this process by aggregating, indexing, and analyzing these machine-generated logs from the RPA system, along with other relevant data sources. This allows for real-time monitoring, detailed searches, and the creation of insightful dashboards and alerts. Essentially, Splunk acts as the primary location for supporting audit trail documents, consolidating RPA bot execution logs, system logs, user activity logs, and security event logs. This centralized approach streamlines audit processes, enhances incident response, and provides a comprehensive view of RPA operations.

16 Is this System listed on As-Built-Architecture (ABA)? If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

Yes

16.1 What is the ABA ID?

212035

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

Enterprise Consolidated Legacy Access Application Programming Interface (ECLAS API)

Incoming/Outgoing

Both

Transfer Method

Other

Other Transfer Method

ECLAS is an undertaking to build and provide an Integrated Middleware, an Enterprise Services platform to access legacy data from mainframe systems. ECLAS exposes web-service access to all the core legacy command core as Generic JavaScript Object Notation (JSON) and Simple Object Access Protocol (SOAP) responses and secured via SITEMINDER using Security and Communication(s) System (SACS) interface, with added benefits of orchestration, Automated Advanced Acquisition (AAA), security, analytics, etc. Key capabilities include service orchestration, data driven parsing and transformations, automated ingestion of mainframe record layouts, and with continuous integration and deployment pipeline for rapid development, build, test, and deployment cycles. ECLAS provides a Service Oriented Architecture based on reusable, scalable Enterprise service, replacement for Local Account Procedure (LAP) service and

eventually migrate the existing LAP consumers, especially applications on non-java platforms.

Interface Type
Forms
Agency Name
Letter 4869C
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Mail

Interface Type
Forms
Agency Name
Sales Order
Incoming/Outgoing
Both
Transfer Method
Mail

Interface Type
IRS Systems, file, or database
Agency Name
UiPath Robotic Process Automation
Incoming/Outgoing
Both
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Taxpayer Assistance Center (TAC) Input Queue/System
Incoming/Outgoing
Both
Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Taxpayer Services Databases
Incoming/Outgoing
Both

Transfer Method
Application to Application (A2A)

Interface Type
IRS Systems, file, or database
Agency Name
Outlook
Incoming/Outgoing
Both
Transfer Method
Secure email/Zixmail

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.
To identify and track any unauthorized access to sensitive but unclassified information and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy, or to detect electronic communications sent using IRS systems in violation of IRS security policy.

SORN Number & Name
IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.
This SORN covers records related to business entities, including Employer Identification Numbers (EINs), business names, addresses, and associated tax account information. The IRS uses this system to manage and maintain business taxpayer accounts. If the automation processes business entities, it uses data covered under this SORN to validate and update business records or create new entities. This ensures accurate maintenance of business taxpayer accounts and supports consistent data across IRS systems.

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 36.003 - General Personnel and Payroll Records

Describe the IRS use and relevance of this SORN.

To administer personnel and payroll programs.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

Mailing, Printing, and Telecommunication Service Management Records

What is the GRS/RCS Item Number?

GRS 5.5 Item 010

What type of Records is this for?

Both (Paper and Electronic)

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

Records of internal mail room, printing/duplication services, and radio/telecommunication services administration and operation.

What is the disposition schedule?

Temporary. Destroy when 3 years old, or 3 years after applicable agreement expires or is cancelled, as appropriate, 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?

Tax Administration - Wage and Investment (W&I) Records

What is the GRS/RCS Item Number?

RCS 29 - Item 1 General Correspondence Files

What type of Records is this for?

Both (Paper and Electronic)

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

This category includes routine correspondence and related documents exchanged between IRS offices, including National, regional, and local offices, concerning service center operations, instructional materials, and organizational or staffing activities. These records document day-to-day administrative communications and do not include materials of significant procedural or organizational importance. Records with long-term reference or historical value are excluded and retained in accordance with IRS records management policies.

What is the disposition schedule?

Destroy 2 years after the end of the year.

Data Locations

What type of site is this?
System
What is the name of the System?
Generalized Integrated IDRS Keying and Research Access Database (GIIKRAD)
What is the sensitivity of the System?
Personally Identifiable Information (PII) including Linkable Data
Please provide a brief description of the System.
An IRS application that provides users with a structured interface to input, research, and manage taxpayer account data within IDRS. It supports data entry, validation, and retrieval activities by standardizing access to IDRS commands and improving efficiency and accuracy in taxpayer account processing.
What are the incoming connections to this System?
Tax analysts are the end-users that have the required access and authority to review taxpayer's data. The system developer and operators are IRS full-time employees (FTEs).
What are the outgoing connections from this System?
The automation exports the data back to IDRS.

What type of site is this?
System
What is the name of the System?
Account Management Service
What is the sensitivity of the System?
Personally Identifiable Information (PII) including Linkable Data
Please provide a brief description of the System.
AMS is a system that obtains taxpayer's information and their previous tax return forms.
What are the incoming connections to this System?
Tax analysts are the end-users that have the required access and authority to review taxpayer's PII data. The system developers and operators are IRS full-time employees (FTEs).

What type of site is this?
System
What is the name of the System?
Integrated Data Retrieval System
What is the sensitivity of the System?
Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.

IDRS holds the taxpayer's information such as their address, name, refund balances, and due balances.

What are the incoming connections to this System?

Tax analysts are the end-users that have the required access and authority to review taxpayer's Personally Identifiable Information (PII) data. The system developer and operators are IRS FTEs.