

Date of Approval: 11/24/2025
Questionnaire Number: 2655

Basic Information/Executive Summary

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

Taxpayer Resources and Unified Services Tier

Acronym:

TRUST

Business Unit

Information Technology

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 Resource and Unified Services Tier (TRUST) is an application platform developed and maintained by the Internal Revenue Service (IRS). The TRUST platform was developed to provide new digital services to taxpayers that streamline and simplify their interactions with the IRS. This platform does not have its own unique system or application components or data processing. It is a container for multiple IRS applications to include Direct File (DFSYS), documented in Privacy and Civil Liberties Impact Assessment (PCLIA) #1925 and Data Authorization and Transfer Service (DATS), documented in PCLIA #2322. TRUST acts as the boundary for these applications hosted within the IRS Integrated Enterprise Portal (IEP) Amazon Web Services (AWS) Cloud.

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).

The applications housed within the TRUST boundary are external-facing applications which provide different services to the Taxpayer for interacting with the IRS. This includes being able to file tax returns directly with the IRS and exporting specific IRS tax data to an external third-party tax preparer. While TRUST itself does not process any PII data, the applications which reside in TRUST will contain FTI and PII as part of their approved application operations.

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

Address

Agency Sensitive Information

Email Address

Employer Identification Number

Family Members

Federal Tax Information (FTI)

Individual Taxpayer Identification Number (ITIN)

Internet Protocol Address (IP Address)

Language

Name

Online Identifiers

Other

Social Security Number (including masked or last four digits)

Tax ID Number

Telephone Numbers

Universal Unique Identifier (UUID)

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

TRUST does not use or process PII as platform. But the applications residing within TRUST use the PII data selected.

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

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)

2

4 Is this a new system?

No

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

No

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.)

TRUST has been created as a boundary for a subset of applications which reside in the IRS IEP AWS GovCloud. While TRUST itself will not process or store sensitive data, the applications within the TRUST boundary do.

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.

WebApps 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.

211884

10 Does this system disclose any PII to any third party outside the IRS?

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.

IRS Integrated Enterprise Portal (IEP) Amazon Web Services (AWS) GovCloud;
06/21/2016; F1603047866

12.2 Does the CSP allow auditing?

Yes

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

3rd party

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)

TRUST is not associated with any processes to access or correct individual information. Any changes or modifications to this data are handled by other IRS business units.

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?

Read only access to logs and monitoring data which may contain PII and SBU.

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.)

Administrators, contractors, and sub-contractors - read only access to logs and monitoring data which may contain PII and SBU. All contractors who support the DATS application have completed an IRS Minimum Background Investigation (MBI) and Public Trust.

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.

TRUST applications use the Privacy Act Statement posted on IRS.gov. 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.

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".

Not Applicable

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

Access to the Integrated Enterprise Portals (IEP) for TRUST application administrators is requested via an IEP enterprise ticketing process. Access is granted on a need-to-know basis. (audit logs and/or IEP data) The enrollment process requires that an authorized manager approve access requests on a case-by-case basis. Access approval is based on the Users role(s) and responsibilities. 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. The employee's access will be terminated once they no longer require access. Access to the data is determined by the System Administrator based on a user's position and need-to-know. The contractors administer the portal/cloud infrastructure, but the SBU/PII is not disseminated to them. Only IRS System Administrators will have access to the production environment. Information requested by the Treasury Inspector General for Tax Administration (TIGTA) must be properly vetted and cleared for release. Access to TRUST applications for external Taxpayers is managed via Secure Access Digital Identity (SADI).

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

No

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

No specific risks have been identified for privacy and civil liberties.

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.

TRUST is not a system or application and therefore does not generate audit trails. TRUST applications have their own individual audit trails. All TRUST application auditing is compliant with IRM 10.8.1 and complete the Enterprise Security Audit Trail (ESAT) worksheet to document all details. Audit logs are captured in IEP Splunk and sent to IRS Splunk for Cyber analysis and alerting, if necessary. TRUST applications do not have any outstanding audit-related Plan of Actions and Milestones (POA&M).

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

IRS IEP AWS GovCloud

Incoming/Outgoing

Both

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Direct File (DFSYS)

Incoming/Outgoing

Both

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Data Authorization and Transfer Service (DATS)

Incoming/Outgoing

Both

Transfer Method

Amazon Web Services Platform (AWS)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 22.062 - Electronic Filing Records

Describe the IRS use and relevance of this SORN.

TRUST applications allows tax filers the ability to file their tax return electronically directly with the IRS and to authorize transfer of their IRS data to third party preparers for the purposes of preparing their tax return.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

RETURNS PROCESSING RECORDS

What is the GRS/RCS Item Number?

29, item 55

What type of Records is this for?

Electronic

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

Electronically Filed Individual, Partnership and Fiduciary Income Tax Returns. Includes all tax returns which are filed with the Service through any type of electronic means.

What is the disposition schedule?

Retire to Records Center beginning January 2 through March 31 following the year in which the returns were numbered and processed. Destroy on or after January 16, 6 years after the end of the processing year unless needed for Collection Statute Expiration Date (CSED) Extract due to a balance due.

Data Locations

What type of site is this?

Environment

What is the name of the Environment?

IRS IEP AWS GovCloud

What is the sensitivity of the Environment?

Sensitive But Unclassified (SBU)

Please provide a brief description of the Environment.

Cloud service provider for the TRUST set of applications.

What are the incoming connections to this Environment?

The incoming connections to the TRUST portion of the IRS IEP AWS GovCloud are Secure Access Digital Identity (SADI) and a secure point-in-time connection between States and/or third-party tax preparers with TRUST applications.

What are the outgoing connections from this Environment?

The outgoing connections from the TRUST portion of the IRS IEP AWS GovCloud are Modernized eFile, participating Direct File States, and third-party tax preparers.