Date of Approval: 06/03/2025
Questionnaire Number: 2322

Basic Information/Executive Summary

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

Data Authorization and Transfer Service

Acronym:

DATS

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.

Data Authorization and Transfer Service (DATS) is a migration of Taxpayer Disclosure Authorization (TDA). DATS provides taxpayers the ability to confirm their identity and authorize the importing of their Adjusted Gross Income (AGI) and Identity Protection Personal Identification Number (IP PIN) by their approved third-party software platform. Taxpayers will login via Secure Access Digital Identity (SADI) and be presented with an option to have their information shared with their selected electronic tax preparer. Once the Taxpayer provides authorization, they are returned to their tax preparation software. At that time, the third-party software platform will authenticate to the IRS via the token provided to them from taxpayer authorization process to retrieve the information authorized to be shared with them (AGI and IP PIN). This will improve the success rate and increase security for individual taxpayers submitting returns through approved 3rd

party software platforms by providing the capability to securely export taxpayer data out of the Internal Revenue Service (IRS). DATS will support identity theft prevention and identification and reduce fraud and rejection during submission processing.

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).

DATS will collect information from the Security Access Digital Identity (SADI)-authenticated Taxpayer to import select Federal Tax Information (FTI) specifically AGI and IP PIN. This data will be presented back to the Taxpayer as part of their third-party preparer authorization. DATS will maintain a record of authorizations provided by the Taxpayer, when the authorization was provided, and the preparer name associated with a particular authorization.

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

Agency Sensitive Information
Email Address
Federal Tax Information (FTI)
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Name
Social Security Number (including masked or last four digits)
Universal Unique Identifier (UUID)

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?

Yes

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

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? (Number)
2

4 Is this a new system?
Yes

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.
Not required

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.
211726

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 is 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.

This system does not disclose any PII to a third parties outside of the IRS. The taxpayer is authorizing the data to be shared to their chosen preparer.

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?

Yes

13.1 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

Yes

13.11 Please upload the approved DIRA report using the Attachments button. Select "Yes" to indicate that you have or will upload the signed DIRA form.

Yes

13.2 If individuals do not have the opportunity to give consent to collect their information for a particular use, why not?

Individuals give consent.

13.3 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

Individuals are notified.

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

DATS only reports back what information the IRS has already collected. 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, IRS-owned and operated with contractors and sub-contractors supporting.

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.

DATS uses 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".

More than 1,000,000

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

Access to the Integrated Enterprise Portals (IEP) for DATS 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 DATS for external Taxpayers is managed via Secure Access Digital Identity (SADI). Only SADI-authenticated users, registered via ID.me, can access DATS to provide authorization to a tax preparer.

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 today 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.

All auditing is compliant with IRM 10.8.1 and DATS is working through the Enterprise Security Audit Trail (ESAT) worksheet on file providing all details. Audit logs are captured in IEP Splunk and sent to IRS Splunk for Cyber analysis and alerting, if necessary. DATS does 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

Electronic Signature Storage and Retrieval Service (ESSAR)

Incoming/Outgoing

Both

Transfer Method

Secured channel via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

Secure Access Digital Identity (SADI)

Incoming/Outgoing

Both

Transfer Method

Secured channel via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

Enterprise Security Audit Trails (ESAT)

Incoming/Outgoing

Both

Transfer Method

Secured channel via HTTPS

Interface Type
IRS Systems, file, or database
Agency Name
Integrated Enterprise Portal (IEP) Amazon Web Service (AWS) GovCloud
Incoming/Outgoing
Both
Transfer Method
Amazon Web Services Platform (AWS)

Interface Type
IRS Systems, file, or database
Agency Name
Enterprise Data Platform (EDP)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Application Programming Interface (API)

Interface Type
IRS Systems, file, or database
Agency Name
Enterprise Consolidated Legacy Access System (ECLAS)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Application Programming Interface (API)

Interface Type
IRS Systems, file, or database
Agency Name
Identity Protection Personal Identification Number (IP PIN)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Application Programming Interface (API)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 22.062 - Electronic Filing Records

Describe the IRS use and relevance of this SORN.

DATS allows tax filers to provide authorization for third party preparers to obtain specific tax information from the IRS on their behalf to prepare and file their tax return electronically via IRS's Modernized eFile (MeF).

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

System and return information collected in accordance with audit, security standards

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

Filed return information is stored against IMF

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?
System
What is the name of the System?
Splunk
What is the sensitivity of the System?
Sensitive But Unclassified (SBU)
Please provide a brief description of the System.
Splunk is primarily used for data analytics, security monitoring, and IT operations management by collecting, analyzing, and visualizing machine-generated data. It helps organizations gain insights, troubleshoot issues, and improve performance across various areas.
What are the incoming connections to this System?
Splunk is the IRS's Security Information and Event Management (SIEM) tool which collects, aggregates, and analyzes log data from various sources within the IRS to detect and respond to security threats in real-time. This integration includes all IRS systems for event monitoring, to include internal operations as well is incoming and outgoing connections.

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)
What is the URL of the item, if applicable?
https://ww4.irs.gov/df/file/dats/home
Please provide a brief description of the Environment.
Cloud service provider for DATS.
What are the incoming connections to this Environment?
The incoming connections to the IRS IEP AWS GovCloud hosting platform for DATS come from the IRS Registered User Portal (RUP). DATS is a public-facing application and as such, all SADI-registered and authenticated Taxpayers have access from their personal computers to DATS, also through the IRS API Public Gateway. Lastly, the integrated third-party tax preparers have access to DATS based on an approved DATS taxpayer authorization and certificate exchange to retrieve select Taxpayer information, if elected by the Taxpayer in support of preparing their federal return.

What are the outgoing connections from this Environment?

The outgoing connections are all bi-directional of the incoming connections. DATS is a public facing application and as such, all SADI-registered and authenticated Taxpayers have access from their personal computers to DATS, also through the IRS API Public Gateway. DATS interacts with the Taxpayer's browser. Lastly, the integrated third-party preparers have access to DATS based on an approved DATS taxpayer authorization and certificate exchange to retrieve select Taxpayer information, if elected by the Taxpayer in support of preparing their federal return.