Date of Approval: 12/10/2025
Questionnaire Number: 2530

Basic Information/Executive Summary

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

Taxpayers and Teletypewriter (TTY)Telecommunication Devices for the Deaf (TDD)

Acronym:

TTY-TDD

Business Unit

Taxpayer Experience Office

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.

Taxpayers and Teletypewriter Telecommunication Devices for the Deaf (TTY/TDD) is a call solution for the hearing impaired used to process an actual TTY/TDD call that connects the caller to a Customer Service Representative (CSR). TTY/TDD is used to make “text calls” over standard phone lines. Taxpayers who use these devices to call the IRS are served via a dedicated telephone number terminating into the IRS’s TTY/TDD equipment which “converses” visually with these taxpayers. TTY/TDD benefits the IRS by helping to achieve its mission by providing call assistance to hearing impaired 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).

TTY/TDD is used to make “text calls” over standard phone lines. Taxpayers who use these devices to call the IRS are served via a dedicated telephone number terminating into the IRS’s TTY/TDD equipment which “converses” visually with these taxpayers. The data shared through TTY/TDD is FTI data and is not stored in the TTY/TDD relay system. It is overwritten upon completion of each call.

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
Federal Tax Information (FTI)
Name
Online Identifiers
Other
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Telephone Numbers

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

IP Addresses, Server Host Names and Server Source Name

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 a process improvement?

No

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

Taxpayer Services and Experience

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)

3

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?

1431

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

Taxpayer and Teletypewriter (TTY) Device for the Deaf (TDD)

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 assessor required changes to the PII listings for all GSS-15 components.

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

Yes

5.1 Identify the parent system's approved PCLIA number.

2501

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

GSS-15 Intelligence Contact Management Network

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.

User and Network Services (UNS)Technical Integration Governance Board (TIB)

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.

211629

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?

No

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?

No

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

The taxpayer has the opportunity to grant consent per IRM 21.2.1.56.

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

IRS policy allows affected parties the opportunity to clarify or dispute negative determinations per the examination appeals process as outlined in IRS Publication 1 - Your Rights as a Taxpayer, and IRS Publication 5 - Your Appeal Rights and How to Prepare a Protest If You Don't Agree. Notice, Consent and Due Process are provided pursuant to 5 USC.

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

No

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.)

Users - read only privileges
Mangers - read and write privileges
System Administrators- administrative privileges

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.

This information is shared audibly with the hearing-impaired taxpayers per the IRM 21.2.1.56 (4).

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".

Under 50,000

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".

Under 5,000

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 is requested via Business Entitlement Access Request System (BEARS). Data access is granted on a need-to-know basis. The BEARS 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. Write, Modify, Delete, and/or Print) are defined on BEARS and set (activated) by the System Administrator prior to the 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 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.

No

24 Explain any privacy and civil liberties risks related to privacy controls.
Privacy controls AU-3(3) POAM IPT0024131 failure to list all applicable PII.
Privacy controls RA-8 POAM IPT0020888 failure to have an approved PCLIA for each component.

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 security audit system tracks elements such as login ID, login date/time, logout date/time, files/directories accessed, attempted security violations, Data from system audit and monitoring files are used to measure system performance including availability, reliability, usability, and resource usage. Additional audit trail data is captured to monitor system access at the operating system level. The audit logs are stored and maintained by the Integrated Automation Technologies (IAT) and Integrated Data Retrieval (IDRS) systems.

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
CCIUP - Infrastructure Upgrade Project - Endpoint Replacement
Incoming/Outgoing
Both
Transfer Method
Secure Data Exchange (SDE)

Interface Type
IRS Systems, file, or database
Agency Name
ICM Finesse- Intelligent Contact Managements Finesse
Incoming/Outgoing
Both
Transfer Method
Secure Data Exchange (SDE)

Interface Type
IRS Systems, file, or database

Agency Name
Humanify Portal with Voss
Incoming/Outgoing
Both
Transfer Method
Secure Data Exchange (SDE)

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.
The security audit system tracks elements such as login ID, login date/time, logout date/time, files/directories accessed, attempted security violations, Data from system audit and monitoring files are used to measure system performance including availability, reliability, usability, and resource usage. Additional audit trail data is captured to monitor system access at the operating system level.

Records Retention

What is the Record Schedule System?
Record Control Schedule (RCS)
What is the retention series title?
IRS Taxpayer Assistance Recorded Quality Control Records
What is the GRS/RCS Item Number?
RCS 31, 24
What type of Records is this for?
Electronic
Please provide a brief description of the chosen GRS or RCS item.
These records are created and maintained for use by managers and reviewers in the Taxpayer Assistance Centers (TAC), Field Sites, and Call Sites. Random recordings of taxpayer/ customer service interface are used to measure and assess customer assistance. Records include audio digital recordings of conversations between IRS assistors and taxpayers who visit a Taxpayer Assistance Center (TAC), and the screen capture images of computer sites used to provide assistance. The records are used to improve the quality of IRS responses to taxpayers. Records are identified by unique identifier of the IRS employee involved in the conversation.

What is the disposition schedule?

Destroy within 18 months when no longer needed for evaluation or documentation purposes.

Data Locations

What type of site is this?

System

What is the name of the System?

Cybersecurity Asset Management (CSAM)

What is the sensitivity of the System?

Federal Tax Information (FTI)

What is the URL of the item, if applicable?

https://csam.int.for.irs.gov/CSAM/Login.aspx

Please provide a brief description of the System.

Is a tool developed and hosted by Department of Justice (DOJ). It supports automation of the NIST Risk Management Framework (RMF). The IRS leverages the CSAM to complete the National Institute of Standards and Technology, Special Publication 800-53, security control assessments and to maintain system security plans throughout the systems' lifecycle.

What are the incoming connections to this System?

DHOH callers may choose the Telecommunications Relay Service (TRS) by calling 711.

What are the outgoing connections from this System?

DHOH callers may choose the Telecommunications Relay Service (TRS) by calling 711.