Date of Approval: 12/17/2025
Questionnaire Number: 2736

Basic Information/Executive Summary

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

GSS-15 - Intelligent Contact Management Network

Acronym:

ICM Intelligent Contact Management Network

Business Unit

IT - Cybersecurity

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 ICM is a component of the General support system -GSS-15 that provides infrastructure support to IRS business applications running on Tier IV (Wintel) platforms and specialized Cisco components at multiple facilities. It provides a combination of services including but not limited to the efficient delivery of taxpayer telephone and teletype contact to trained assistors in the various contact centers and automatic response centers in the Contiguous United States (CONUS) and Puerto Rico. ICM is also connected to other computing centers through IRS backbone infrastructure

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).

Social security numbers are requested but not stored in ICM. Standard Employee Identifier (SEID) and Automatic Number Identification (ANI) are captured in the logs but are purged after 14 days Intelligent Contact Management (ICM) networks use Automatic Number Identification (ANI) to identify and use a caller's phone number to enhance customer service and streamline contact center operations. Unlike standard caller ID, ANI is more reliable and cannot be blocked by the caller because the phone number data is transmitted directly through the telecommunications network. When a customer calls a contact center that uses an ICM network, ANI data provides the system with critical information to inform intelligent routing decisions and give agents a full view of the customer's history.

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

Document Locator Number (DLN)
Employer Identification Number
Other
Social Security Number (including masked or last four digits)

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

Device name and IP Address

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

Information by CI for certain money laundering cases - 18 USC
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
PII for personnel administration - 5 USC

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)?

Application

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?
Yes

4.11 What is the previous PCLIA number?
2501

4.12 What is the previous PCLIA title (system name)?
GSS-15 - Intelligent Contact Management Network (ICM)

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.)
Privacy requires all possible PII that will be shown in the scan and in the application be listed, which are Name, SEID, Device Name and IP address.

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

5.1 Identify the parent system's approved PCLIA number.
PCLIA 2450

5.2 Identify the parent system's name as previously approved.
GSS-15 Main

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

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.

#211329

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?

No

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)

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.)

User: Read only Manager: Read and write System admins: Administrator Access Level: Read Only, Read and Write, or an Administrator, background investigations are conducted for all contractors. The attachment shows the level of background investigation.

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.

Privacy Act Statement is not used, and individuals are not given the opportunity to consent to the collection of their PII. This system uses PII obtained by other systems and does not collect PII on its own nor does it interact with the public directly

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".

IRS Employees 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".

Contractors 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".

Not Applicable

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

Account access is managed through the Business Entitlement Access Request System, (BEARS) Entitlement process. Appropriate approvals at several levels are required to grant access to components within GSS-15.

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.

PT-05, Privacy Notice - and AU-03(3) Limit Personally Identifiable Information Elements are the Open Plan of actions and milestones (POAMs) related to Privacy that needs to be remediated. GSS-15 Components failed to limit Personally Identifiable Information (PII) elements in the audit logs to those identified in the approved PCLIA.

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.

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
ICM -Intelligent Contact Management Network
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Secured channel via HTTPS

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?
Non-Record
What type of Records is this for?
Both (Paper and Electronic)
Please provide a brief description of the chosen GRS or RCS item.
IDRS is an access or computer application, infrastructure or interface. IDRS does not create, store, and/or manage records as defined under the Federal Records Act (44 U.S.C.) and does not need to be scheduled. Any data within the system itself is

considered duplicative of data derived from other systems. The data which is passed through by IDRS is not archived and IDRS itself does not maintain a data log or audit information. Applications that interface with IDRS and have data storage, tracking, and audit information are scheduled and/or will be scheduled independent of IDRS.

Data Locations

What type of site is this?

System

What is the name of the System?

Cyber Security Assessment and management (CSAM)

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

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.

CSAM - 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.