

Date of Approval: 06/13/2025
Questionnaire Number: 2353

Basic Information/Executive Summary

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

IRS Customer Relationship Management - Phoenix - Salesforce

Acronym:

IRSCRM-TAS

Business Unit

National Taxpayer Advocate Service

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 IRS Customer Relationship Management (IRSCRM) will be used for managing relationship between IRS, Taxpayers, other government entities. This is an ongoing phased integration, with Taxpayer Advocate Service being one of the first organizations to track their cases, including Integrated Data Retrieval System (IDRS) and Account Management Services (AMS) integrations. Anticipated summer deployment of 2025. Data will be used to facilitate case assignment, project assignment, and routing processes which provide access to the correct individuals and teams. This allows them to access and retrieve details about cases from integrated sources. Applicable approvals will be captured and/or required to assist in consistent documentation development. Enhanced case management capabilities facilitate easier case resolution through improved assignment, action tracking and clearer visibility into deadline expectations. Real-time, and user-

specific, reporting will provide insight into capacity/workload management and new, outstanding, and completed cases. Existing data, captured via manual entry or integration, will be leveraged throughout the lifecycle of a case.

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 (SSNs) are stored in IRSCRM and will be used to look-up taxpayer and case information (as identified in the IRS/Treasury System of Records Notices' (SORNs') routine uses); this allows for seamless integration with other IRS systems. The IRSCRM system requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer at this time. The use of SSNs is permissible from Internal Revenue Code (IRC) 6109. The system contains or will contain records that are covered under the General Records Schedule (GRS, IRS Document 12829), or has a National Archives and Records (NARA) archivist approved a Records Control Schedule (RCS, IRS Document 12990). The following information reflects the different records and the approved dispositions (retention and destruction of official agency records) for the records to be stored in this system.

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

Address

Centralized Authorization File (CAF)

Email Address

Employer Identification Number

Individual Taxpayer Identification Number (ITIN)

Language

Name

Social Security Number (including masked or last four digits)

Standard Employee Identifier (SEID)

Tax ID Number

Telephone Numbers

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

SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this a new system?

No

1.1 Is there an approved Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

Yes

1.11 Has the name changed since the prior PCLIA?

Yes

1.12 What is the System Name on the most recent approved PCLIA?

IRS Customer Relationship Management

1.13 What is the Acronym on the most recent approved PCLIA?

IRSCRM

1.2 What changes occurred to require this updated PCLIA?

CRM added new use cases to the Salesforce Platform since the original PCLIA.

These use cases will be creating their own PCLIA's to cover their applications.

This PCLIA is specific to the Phoenix application.

2 What is the name of the contractor?

Salesforce Professional Services

3 Please provide a contact person for the contractor.

XXXXX

4 Please provide the phone number for the contractor.

XXXXX

5 What is the email address for the contractor?

XXXXXX

6 What is the address for the contractor?

XXXXX XX

7 What is the location of the contractor?

Remote

8 What is the contract number?

NNG15SD29B

9 What is the length of the contract?

Base Period: 12 months

10 What is the contract start date?

3/1/2025

11 What is the contract end date?

2/28/2026

12 What is the Contracting Officer (CO) name?

XXXXXX

13 What is the CO's email address?

XXXX

14 What is the CO's phone number?

XXX

15 Who is the Contracting Officer's Representative (COR)?

XXXXXX

16 What is the COR's email address?

XXXXXXX

17 What is the COR's phone number?

XXXX

18 What is the IRS business unit procuring the contract?

Enterprise Services - Technology Strategy Management (ES TSM)

19 What is the business owner contact name?

XXXXXXXXXX

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

Access to the IRSCRM is requested using Business Entitlement Access Request System (BEARS). 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. 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. The primary Cloud Service Provider (Salesforce/ MuleSoft) administrators have a High-level background investigation.

21 Are any authorized employees approved for telework?

Yes

21.1 Is there an approved telework agreement/policy?

Yes

22 Describe the work to be performed, how PII will be used, collected, received, displayed, stored, maintained, or disseminated.

Yes

23 Provide a clear, concise reason why the contractor will use the PII, the benefit to IRS, and how the information will be used.

Salesforce will use PII data to accurately identify taxpayers and associate them with TAS Case Advocacy and Systemic Advocacy cases. Proper identification will facilitate faster resolution of cases and issues, ultimately enhancing taxpayer satisfaction.

24 Please indicate the location where the work will be performed, and how the data will be processed, stored, and secured.

Work will be done in the United States. Data will be stored and processed in the Salesforce Gov cloud which is FedRAMP approved.

25 Is any data accessed, processed and/or stored outside the United States or US Territories?

No

26 Describe the procedures for agency oversight on contractor, access, storage, and destruction of PII, disclosure awareness training and incident reporting.

Standard IRS/government clearance vetting procedures. Access is granted through BEARS entitlement(s) after contractors have completed required FISMA training. Storage and destruction of PII, disclosure awareness training, and incident reporting is followed in accordance with standard IRS policies and procedures.

27 If applicable, what is the IRS PCLIA Number for the system that is providing the information associated with this contract?

8512

28 Are you receiving only the data that is needed to accomplish the task?

Yes

29 From what sources are you obtaining data (other than the IRS) to fulfill this contract?
None

30 Do you have subcontractors who work on the contract?
No

31 Does this system use Artificial Intelligence (AI)?
No

32 Does the system use cloud computing?
Yes

32.1 Please identify the Cloud Service Provider (CSP).
Salesforce FedRAMP ID: FR2003061248 MuleSoft ID: FR1818161169

32.2 Is the CSP FedRAMP Authorized?
Yes

32.3 Privacy laws (including access and ownership) can differ in other countries. Does the data physically reside in systems located in the United States and its territories and is all access and support of this system performed from within the United States and its territories?
Yes

33 Who owns and operates the system (IRS Owned and Contractor Operated, Contractor Owned and Operated)?
Salesforce, as the Cloud Services Provider “owns” the platform, however the configuration, customizations & data remains the IRS’s as it is a SaaS cloud application.

34 Identify the roles and their access level to the PII data. Indicate whether background investigations are complete or not.
Business Entitlement Access Request System (BEARS) entitlements outline roles and access levels. All background investigations are complete.

35 Describe the system's audit trail in detail.
Salesforce and MuleSoft have built-in auditing capabilities and Enterprise Security Audit Trails (ESAT) auditing recommendations will be configured. Splunk will periodically pull platform and application audited events and process them. During upcoming phases, we will provide audit log information which will include trackable events and schedule of audits; for example, the SBU/PII elements contained in audit log(s), types of data, and tracking events for the system.

36 Does this system use, or plan to use SBU Data in a non-production environment?
Yes

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

AMS

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Secured channel via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

TAMIS

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Other

Other Transfer Method

Kiteworks/Secure transfer via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

IDRS

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Secured channel via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

BPMS

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Other

Other Transfer Method

Secure transfer via HTTPS/Secure file transfer protocol (SFTP)/Kiteworks

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 00.003 - Taxpayer Advocate Service and Customer Feedback and Survey Records

Describe the IRS use and relevance of this SORN.

This data is used for Tax Administration and case inventory and tracking purposes. (Legal advice determinations, storage and reference of case inventory statuses.)

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Taxpayer Advocate

What is the GRS/RCS Item Number?

RCS 16 Item 9a

What type of Records is this for?

Electronic

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

Records whether studies, analyses or correspondence, which established the policies, practices and programs for the management of the Taxpayer Advocate Service organization. Included are organizational changes, functional realignments and responsibilities, and long and short-range planning documents.

What is the disposition schedule?

Cut off correspondence annually, studies and case files upon completion of study or at appropriate phase. Retire to Records Center 5 years after cutoff, or when no longer needed. Transfer to NARA 15 years after cutoff.

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Customer Service

What is the GRS/RCS Item Number?

RCS 31 Item 94

What type of Records is this for?

Both (Paper and Electronic)

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

Taxpayer Advocate Management Information System (TAMIS).

The Taxpayer Advocate Management Information System (TAMIS) is an automated, computerized application used to record, control, process, analyze, and report on Taxpayer Advocate Service (TAS) case inventories. It also maintains a data repository for report generation.

What is the disposition schedule?

(A) Inputs: Taxpayer Advocate Service (TAS) staff input information into the Taxpayer Advocate Management Information System (TAMIS) derived from direct communication through the telephone, FAX, mail, e-mail, or walk-in/face-to-face contacts, and IR Form 911, Request for Taxpayer Assistance Order, or an E-911 (Electronic Form 911) from Accounts Management Services (AMS). (GRS 5.2, item 020; Job No. DAA-GRS-2017-0003-0002) AUTHORIZED DISPOSITION Delete/Destroy all cached records after successful entry and verification. (B) System Data: Contents of the Taxpayer Advocate Management Information System (TAMIS) include, but are not limited, to the following: Taxpayer Information (Social Security Number or other Taxpayer Identification Number, name, Address; The Executor's/Power of Attorney's name, address, phone number; tax issue, etc.), Employee Information (Staff Employee Identification Number, Post of Duty, Address, Telephone Number, etc.), Audit Trail Information, and Case Management Information. (Job No. N1-58-09-81) 1. Case Management Database. AUTHORIZED DISPOSITION Cut off at end of the fiscal year in which case is closed. Delete/Destroy 3 years after cutoff. 2. Audit Log Database. AUTHORIZED DISPOSITION Cut off at end of the fiscal year in which case is closed. Delete/Destroy 7 years after cutoff, or when no longer needed for operational purposes, whichever is later. (C) Outputs: Outputs from the Taxpayer Advocate Management Information System (TAMIS) include case management data which can be transmitted or viewed on the desktop, and reports that can be printed daily. In addition, the Business Performance Management System (BPMS) via Business Objects software extracts key statistical measures from TAMIS monthly. (GRS 5.2, item 020; Job No. DAA-GRS2017-0003-0002) AUTHORIZED DISPOSITION Delete/Destroy when no longer needed for operational purposes.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2 System Access Records

What is the GRS/RCS Item Number?

GRS 31

What type of Records is this for?

Electronic

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

These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: user profiles, log-in files, password files, audit trail files and extracts, system usage files, cost-back files used to assess charges for system use Systems requiring special accountability for access. These are user identification records associated with systems which are highly sensitive and potentially vulnerable.

What is the disposition schedule?

Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

3.2 System Access Records

What is the GRS/RCS Item Number?

GRS 30

What type of Records is this for?

Electronic

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

These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as: user profiles, log-in files, password files, audit trail files and extracts, system usage files cost-back files used to assess charges for system use Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users.

What is the disposition schedule?

Temporary. Destroy when business use ceases.

Data Locations

What type of site is this?

System

What is the name of the System?

SalesForce

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

What is the URL of the item, if applicable?

<https://ccirsgov.lightning.force.com/>

Please provide a brief description of the System.

The IRS Customer Relationship Management (CRM) System is a cloud hosted Software as a Service (SaaS) solution hosted in AWS GovCloud. The CRM Platform consists of Salesforce (application layer) and MuleSoft (integration layer) components. CRM Products are managed and configured by Platform tenants according to their business use cases. The CRM Platform provides reusable infrastructure and foundational services for products, including single-sign-on enablement, audit and event logging, and CI/CD pipeline management.

What are the incoming connections to this System?

Incoming connections to this system: Active Directory Federation Services, IRS Gitlab, AMS, TAMIS data (via Kiteworks -one time data migration).

What are the outgoing connections from this System?

Outgoing Connections from this system: IRS Splunk, ECLAS APIs (IDRS), BPMS (via Kiteworks).