

Date of Approval: 02/17/2026
Questionnaire Number: 2648

Basic Information/Executive Summary

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

IRS Customer Relationship Management - Congressional Portal - Salesforce

Acronym:

IRSCRM-IRSCP

Business Unit

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 is deploying the Salesforce Customer Relationship Management (CRM) platform in an ongoing, phased project. The Taxpayer Advocate Service (TAS) was one of the first organizations to use it with an implementation called Phoenix, which has approved PCLIA 2353, IRS Customer Relationship Management - Phoenix - Salesforce. This Congressional Portal builds on and leverages the functionality of Phoenix to enable congressional staffers at the U.S. House and U.S. Senate to request TAS assistance for their constituents. Congressional requests are worked by TAS. This will replace the cumbersome manual submission and subsequent processing of Form 911, Request for Taxpayer Advocate Service Assistance, which is the current method. Access to the IRS Congressional Portal will be automatically granted to congressional staffers based on credentials provided by the U.S. House and U.S. Senate Active Directory

systems via the Just-in-Time (JIT) provisioning/Single-Sign-On (SSO) flow. That data source confirms the user is an active member of a congressional office, leveraging active monitoring by House and Senate IT/Security teams to grant and revoke access. The congressional systems will interact with the IRS's Active Directory Federation Services (ADFS) to control access to the Congressional Portal. This CRM allows the IRS to securely and automatically control the initial requests and captures all resulting case activity, while also providing congressional staffers with the ability to constantly monitor case progress. Another benefit to the IRS will be the standardization of case documentation within the portal. Congressional staff will be notified via email once a request is finalized. The system owner is the Internal Revenue Service (IRS), which maintains overall authority and responsibility for the system. The system is operated with contractor support from Salesforce, which provides the hosted platform and related services in accordance with contractual requirements and IRS oversight.

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).

Entries to this system may contain Federal Tax Information (FTI) and Personally Identifiable Information (PII) as listed below. House and Senate Congressional Aides use the IRS Congressional Portal to submit information which will be ingested and used to create cases within the Phoenix application and look up case information, consistent with the uses outlined in IRS/Treasury System of Records Notifications. Requests that contain Federal Tax Information (FTI), such as SSNs or EINs, as well as Personally Identifiable Information (PII), are stored in CRM dataset. PII is shared outside the IRS with approved third-party systems, including DAWSON and SPLUNK, for authorized logging, monitoring, and operational purposes, in accordance with IRS security and privacy requirements. Salesforce contractor personnel have Administrator access to perform platform administration and operational support. Access is role-based, limited to the minimum necessary, and subject to IRS oversight and security controls. The IRS Congressional Portal will send email notifications to both internal IRS users and external portal users. When a file is no longer required, a user may perform a soft delete, which transfers the file to the platform's Recycle Bin. Salesforce retains soft-deleted items in the Recycle Bin for 15 days, after which the system automatically performs a permanent deletion. These notifications will be secured with a DomainKeys Identified Mail (DKIM) signature.

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
Federal Tax Information (FTI)
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Language
Name
Other
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number
Telephone Numbers

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

Congressional Office assignment Spouse Information

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?

Yes

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

Taxpayer Advocate Service (TAS)

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?

Yes

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

Yes

5.1 Identify the parent system's approved PCLIA number.

8512

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

IRS Customer Relationship Management (IRSCRM)

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?

Yes

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

Technology Strategy Mgmt is over CRM; Taxpayer Advocate Service
Technology Executive Governance Board (TEGB)

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.

CRM (parent) number 211526; Phoenix is 211904

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

Yes

10.1 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?

Yes

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

Salesforce FedRAMP ID: FR2003061248 05/27/2020; MuleSoft ID:
FR1818161169 07/31/2019

12.2 Does the CSP allow auditing?

Yes

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

Yes, IRS (CRM and Cybersecurity)

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

Moderate (High for Salesforce parent)

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)

Taxpayer FTI input by congressional offices is not editable in the CRM. Due process to address federal tax deficiencies is afforded by the Internal Revenue Code and established IRS tax administration procedures, not directly through the CRM. Any error would be corrected in accordance with Taxpayer Advocate procedures and posted in Phoenix or other IRS systems as appropriate.

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?

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.)

IRS Employees: --- Users: Read and Write for FTI

IRS Managers: Read and Write for FTI

IRS and contracted Sys. Administrators: Administrator

IRS and contracted Developers: Administrator

All contracted staff with access have Public Trust background investigations completed and approved. Administrator access is "High"

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 U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!

WARNING: By accessing and using this U.S. government computer system, you are consenting to system monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities, including detection and prevention of any unauthorized use of this system. The system you are accessing may contain confidential tax information and is designed exclusively for use by authorized persons to interact with the IRS and retrieve confidential tax information using only their own account. Any other use of this system that is inconsistent with the intended purposes of the system is an unauthorized use of the system and strictly prohibited.

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".

Not applicable; contractors are not system users except as a member of the public.

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".

Currently 100,000 to 1,000,000 (about 250k added annually)

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

User administration records: under 10,000

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

Access to the IRS Congressional Portal will be automatically granted to congressional aides in the U.S. House and Senate based on information provided by the U.S. House and U.S. Senate Active Directory systems via the JIT/SSO flow. This data confirms whether a user is an active member of a congressional office. Since House and Senate IT/Security teams actively monitor and promptly revoke access in Active Directory when a staffer leaves an office, the IRS can rely on this mechanism without requiring additional manual vetting. As a result, access to office-specific congressional requests and related communications will be securely and automatically controlled based on current ADFS records. Access to the IRSCRM-TAS is requested using the 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) administrators have a High-level background investigation; the third-party contractor (MuleSoft) has less access privileges, so they have a Moderate-level background investigation.

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

Yes

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

There are some typical risks to cloud-based systems, related to known/approved users seeing more data than intended through (1.) elevated permissions by having records shared directly with user by another user, and (2.) incorrect group membership by easily rectifiable mistakes by administrators. All applicable system assessments have been/will be performed, and risks mitigated accordingly/appropriately/to the extent possible.

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.

Salesforce and MuleSoft have built-in auditing capabilities and 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. Activities of internal IRS users and external congressional aides are going to be exported to Splunk.

27 Does this system use or plan to use SBU data in a non-production environment?

Yes

27.1 Please upload the Approved Email and one of the following SBU Data Use Forms, Questionnaire (F14664) or Request (F14665) or the approved Recertification (F14659). Select Yes to indicate that you will upload the Approval email and one of the SBU Data Use forms.

Yes

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

U.S. House and U.S. Senate Active Directory (ADFS)

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Other

Other Transfer Method

Lightweight Directory Access Protocol (LDAP)

Interface Type

IRS Systems, file, or database

Agency Name

Active Directory Federation Services

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Other

Other Transfer Method

Lightweight Directory Access Protocol (LDAP)

Interface Type

IRS Systems, file, or database

Agency Name

Enterprise Security Audit Trail (ESAT)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Other

Other Transfer Method

Splunk Universal Forwarder

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.

Congressional Portal audit records are sent to Splunk via CRM.

SORN Number & Name

IRS 00.001 - Correspondence Files and Correspondence Control Files

Describe the IRS use and relevance of this SORN.

TAS Congressional Portal maintains correspondence and related records generated when taxpayers seek assistance from their congressional representatives on matters within IRS jurisdiction.

SORN Number & Name

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

Describe the IRS use and relevance of this SORN.

TAS will use records for customer satisfaction communications with congressional offices, the data for identifying customer sat targets (people who we might survey) comes from TAS cases.

Records Retention

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.

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 on a monthly basis. (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?

Record Control Schedule (RCS)

What is the retention series title?

Taxpayer Advocate

What is the GRS/RCS Item Number?

RCS 16 Item 10

What type of Records is this for?

Electronic

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

Records include correspondence with Congress, commissions mandated by Congress, other Federal agencies, state and local governments, questionnaires, internal memorandums; final reports; surveys; test results; publications; and implementation plans

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.

Data Locations

What type of site is this?

System

What is the name of the System?

IRS CRM Congressional Portal-PROD

What is the sensitivity of the System?

Federal Tax Information (FTI)

What is the URL of the item, if applicable?

<https://ccirsgov.my.salesforce.com>

Please provide a brief description of the System.

The IRS is deploying the Salesforce Customer Relationship Management (CRM) platform in an ongoing, phased project. The Taxpayer Advocate Service (TAS) was one of the first organizations to use it with an implementation called Phoenix, which has approved PCLIA 2353, IRS Customer Relationship Management - Phoenix - Salesforce. This Congressional Portal builds on and leverages the functionality of Phoenix to enable congressional staffers at the U.S. House and U.S. Senate to request TAS assistance for their constituents. Congressional requests are worked by TAS. This will replace the cumbersome manual submission and subsequent processing of Form 911, Request for Taxpayer Advocate Service Assistance, which is the current method. Access to the IRS Congressional Portal will be automatically granted to congressional staffers based on credentials provided by the U.S. House and U.S. Senate Active Directory systems via the Just-in-Time (JIT) provisioning/Single-Sign-On (SSO) flow. That data source confirms the user is an active member of a congressional office, leveraging active monitoring by House and Senate IT/Security teams to grant and revoke access. The congressional systems will interact with the IRS's Active Directory Federation Services (ADFS) to control access to the Congressional Portal. This CRM allows the IRS to securely and automatically control the initial requests and captures all resulting case activity, while also providing congressional staffers with the ability to constantly monitor case progress. Another benefit to the IRS will be the standardization of case

documentation within the portal. Congressional staff will be notified via email once a request is finalized.

What are the incoming connections to this System?

Active Directory Federation Services, IRS Gitlab

What are the outgoing connections from this System?

IRS ESAT

What type of site is this?

System

What is the name of the System?

IRS CRM Congressional Portal-LAB

What is the sensitivity of the System?

Federal Tax Information (FTI)

What is the URL of the item, if applicable?

<https://ccirsgov.my.salesforce.com>

Please provide a brief description of the System.

The IRS is deploying the Salesforce Customer Relationship Management (CRM) platform in an ongoing, phased project. The Taxpayer Advocate Service (TAS) was one of the first organizations to use it with an implementation called Phoenix, which has approved PCLIA 2353, IRS Customer Relationship Management - Phoenix - Salesforce. This Congressional Portal builds on and leverages the functionality of Phoenix to enable congressional staffers at the U.S. House and U.S. Senate to request TAS assistance for their constituents. Congressional requests are worked by TAS. This will replace the cumbersome manual submission and subsequent processing of Form 911, Request for Taxpayer Advocate Service Assistance, which is the current method. Access to the IRS Congressional Portal will be automatically granted to congressional staffers based on credentials provided by the U.S. House and U.S. Senate Active Directory systems via the Just-in-Time (JIT) provisioning/Single-Sign-On (SSO) flow. That data source confirms the user is an active member of a congressional office, leveraging active monitoring by House and Senate IT/Security teams to grant and revoke access. The congressional systems will interact with the IRS's Active Directory Federation Services (ADFS) to control access to the Congressional Portal. This CRM allows the IRS to securely and automatically control the initial requests and captures all resulting case activity, while also providing congressional staffers with the ability to constantly monitor case progress. Another benefit to the IRS will be the standardization of case documentation within the portal. Congressional staff will be notified via email once a request is finalized.

What are the incoming connections to this System?

Active Directory Federation Services, IRS Gitlab

What are the outgoing connections from this System?
IRS ESAT