Date of Approval: 10/30/2025
Questionnaire Number: 2678

Basic Information/Executive Summary

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

CI CAF Compromise

Acronym:

CI

Business Unit

Criminal Investigation

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.

This Robotic Process Automation (RPA) attended solution, Criminal Investigation (CI) Centralize Authorization File (CAF) Compromise, is owned by CI and developed on a CI-issued computer utilizing the CI network and CI credentials. The only individual(s) who will have access to this attended automation are Special Agents that receive CAF referral emails from suspected CAFs that have been compromised. This RPA will automate the current manual process of notifying customers whose CAF numbers are suspected of being compromised. The user will run the automation after receiving an email with a distribution list of potentially compromised authorizations. The automation then extracts key information-such as CAF numbers and customer names from an attached excel file within the email and logs it into the "CAF Tracking Dashboard" Excel file stored in a designated CAF SharePoint folder. The file is

then downloaded from SharePoint and saved to a folder in a shared drive location. A blank 9814 document is opened and populated with the affected customers information. A new email is also created and includes the 9814 document, the verification letter, and previously downloaded excel file and is sent out to the affected customers, informing them of the potential compromise and instructing them to submit notarized identification by mail or email for verification. PII involved in this current manual process includes: the client's first and last name, their Social Security Number (SSN), Employer Identification Number (EIN), CAF holder and Power of Attorney (POA)'s number, CAF holder/POA's address, and their telephone number. PII is also used to create the name of the Shared drive folder for sorting documentation. The content of the 9184 document and client's information is also saved in this folder. For the receipt of Notary form, PII includes driver's license and its information, telephone number, and email of the CAF Holder/POA. The PII of the client(s) is redacted using Excel Macro and is sent via email to CAF holder/POA. All aspects of the automation, including input and outputs, are stored on the CI Special Agent's CI-issued laptop throughout the entire attended automation run.

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).

This automation uses data that is contained locally on the CI Special Agent's CI-issued laptop. The automation uses the Special Agent's credentials and access to the CI CAF Outlook shared inbox, CAF Tracking SharePoint site, and the CAF Comp Network shared drive. The automation will monitor the CI CAF Outlook inbox for incoming CAF referrals, access the CAF file folder and create a template for a new entry in the CAF Tracking Dashboard, including the client's CAF#, name, Address, status, and referral date sent. The automation will then create a Mail Merge file of the new CAF referral. The automation will then create a redacted file of relevant referral and send redacted file to POA/Tax Practitioner. The automation will utilize shared resource folder template to send an email to CAF unit notifying them if there was a CAF compromise.

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

Driver's License Number
Email Address
Employer Identification Number

Federal Tax Information (FTI)
Name
Preparer Taxpayer Identification Number (PTIN)
Social Security Number (including masked or last four digits)
Tax ID Number
Telephone Numbers

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
PII about individuals for Bank Secrecy Act compliance - 31 USC
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 process improvement?
No

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

2 Describe in detail, the Robotic Process Automation (RPA) process; be sure to identify the project title and business unit owner; state what IRS Strategy or initiative it supports; identify the system or process it supports and if PII will be required for the RPA to run; identify activities and workflow controls with the type and capabilities that will be incorporated; lastly indicate how the service benefits from the use of this RPA. (Process, Library, Test Automation, Template.)
This Robotic Process Automation (RPA) attended solution, Criminal Investigation (CI) Centralize Authorization File (CAF) Compromise, is owned by CI and developed on a CI-issued computer utilizing the CI network and CI credentials. The only individual(s) who will have access to this attended automation are Special Agents that receive CAF referral emails from suspected CAFs that have been compromised. This RPA will automate the current manual process of notifying customers whose CAF numbers are suspected of being compromised. The user will run the automation after receiving an email with a distribution list of potentially compromised authorizations. The automation then extracts key information-such as CAF numbers and customer names from an attached excel file within the email and logs it into the "CAF Tracking Dashboard" Excel file stored in a designated CAF SharePoint folder. The file is then downloaded from SharePoint and saved to a folder in a shared drive location. A blank 9814 document is opened and populated with the affected customers information. A new email is also created and includes the 9814 document, the verification letter, and previously downloaded excel file and is sent out to the affected customers, informing them of the potential compromise and instructing them to submit notarized identification by mail or email for verification. PII involved in this current manual process includes: the client's

first and last name, their Social Security Number (SSN), Employer Identification Number (EIN), CAF holder and Power of Attorney (POA)'s number, CAF holder/POA's address, and their telephone number. PII is also used to create the name of the Shared drive folder for sorting documentation. The content of the 9184 document and client's information is also saved in this folder. For the receipt of Notary form, PII includes driver's license and its information, telephone number, and email of the CAF Holder/POA. The PII of the client(s) is redacted using Excel Macro and is sent via email to CAF holder/POA. All aspects of the automation, including input and outputs, are stored on the CI Special Agent's CI-issued laptop throughout the entire attended automation run.

3 Is this a new Robotic Process Automation (RPA) project?

Yes

4 Identify the IRS IT systems, applications, projects, and/or databases this RPA is applied to; include the associated system name.

UiPath IT RPA, Microsoft 365, Shared Mailbox for CI CAF, CAF Tracking SharePoint, CAF Comp Network Share drive

5 Identify why the use of SBU/PII/FTI is required; include any type of Sensitive But Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI) that this project will create, collect, receive, use, process, maintain, access, inspect, display, store, disclose, disseminate, or dispose of.

This automation requires the use of SBU/FTI/PII as the CI CAF Compromise process directly involves dealing with client/CAF holder/POA data. All SBU/PII/FTI data will be processed on the CI-issued laptop on the CI network. Only Special Agents with access on the CI CAF team will have access to this automation, as they are the only ones with the necessary credentials the bot uses to access the Shared Mailbox for CI CAF, CAF Tracking SharePoint, CAF Comp Network Share drive. This attended automation will not store any data on the user's machine, as data is located in Shared Mailbox for CI CAF, CAF Tracking SharePoint, CAF Comp Network Share drive.

6 Is your RPA Attended/Unattended?

This is an attended automation.

7 Is this RPA process converting from paper to electronic format or automating a process currently performed by a human?

Yes

7.1 Explain the process being replaced/automated.

Yes

8 Indicate what level of complexity the RPA is classified as and if you were required to register with One Solution Delivery Lifecycle (OneSDLC) or not, or indicate if Information Technology's (ITs) Technical Insertion process was used for approval of this RPA.

This automation is classified as medium complexity.

9 Will connections or interdependencies be established for this RPA?

Yes

9.1 Will the connection be encrypted?

Yes

9.2 Will authentication/credentials be required?

Yes

9.3 Please provide details for the connection/interdependency. Indicate if this occurs on the backend versus through the system/user interface.

The dependencies of this automation are: UiPath IT RPA, Microsoft 365, Shared Mailbox for CI CAF, CAF Tracking SharePoint, CAF Comp Network Share drive. No custom implementations will be used for this automation.

10 Indicate who has or will have permission to access the data and how users are authenticated.

The following people have access to this application- IRS CI CAF authorized users and IRS CI approved contractors authorized to execute the application.

11 Indicate if Business Entitlement Access Request System (BEARS) entitlements are required for access and if Privileged User Management Access System (PUMAS) control management is applied for granting access to the system(s)? If BEARS/PUMAS are not applied, indicate what access controls are in place.

BEARS entitlements are required for this automation. BEARS entitlements are needed for access to the CI UiPath tenant and for the CI production environments.

12 Identify the maintenance tasks or updates performed; state whether or not the maintenance tasks are inherited from the host (UiPath Platform) or you are using customized maintenance activities.

This automation is being built and maintained by the IT RPA (UiPath Platform) team. IT RPA will be responsible for any Operation & Management (O&M) defects, system updates, maintenance, etc. as needed.

13 Indicate if this product or system shares data outside of the United States or its territories.

No

14 Indicate if this system or Robotic Process Automation (RPA) is trained through the use of algorithms; indicate if the algorithm used contains data with a sensitivity classification. (Sensitive but unclassified data might include algorithms, methods, system data, or PII/FTI that could be used to re-identify a person.)

No

15 Describe this system's (RPAs) audit trail process in detail; include location of supporting documents (SPLUNK). Note: Upload of this document is required.

UiPath provides the audit trails at the organization/tenant level, and these logs are stored in mssql database. UiPath also provides an integration to external log products like SPLUNK. And managed service uses SPLUNK as the log aggregator, and all the UiPath logs are fed into Integrated Enterprise Portal (IEP) SPLUNK and IEP SPLUNK is connected to IRS SPLUNK. Any logs going to IEP SPLUNK will be forwarded to IRS SPLUNK. Location for Integrated Enterprise Portal (IEP) SPLUNK is as follows: Integrated Enterprise Portal (IEP) Splunk hostname: https://laco-irs.mgt.afsiep.net/ Index: service_fabric_prod Source: rancher:uipath:audit.

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

CAF Comp Network Shared Drive

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

Forms

Agency Name

CAF Mail Merge File

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Application to Application (A2A)

Interface Type

IRS Systems, file, or database

Agency Name

CAF Tracking SharePoint

Incoming/Outgoing

Incoming (Receiving)

Transfer Method
Secured channel via HTTPS

Interface Type
IRS Systems, file, or database

Agency Name
CI CAF Shared Outlook Inbox
Incoming/Outgoing
Both
Transfer Method
Application to Application (A2A)

Interface Type
Forms
Agency Name
Final CAF Processing File
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Application to Application (A2A)

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 24.030 - Customer Account Data Engine Individual Master File
Describe the IRS use and relevance of this SORN.
Client/taxpayer individual information is accessed as a result of the CI CAF Compromise Process

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
To identify and track any unauthorized accesses to sensitive and classified information and potential breaches.

Records Retention

What is the Record Schedule System?
Record Control Schedule (RCS)

What is the retention series title?

Power of Attorney (POA)/Tax Information Authorization (TIA), Centralized Authorization File (CAF)

What is the GRS/RCS Item Number?

RCS 29 Series 54

What type of Records is this for?

Both (Paper and Electronic)

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

Authorization for a third party to act on behalf of a taxpayer before IRS or to receive or inspect certain tax information for the taxpayer. (1) POAs and TIAs (Hard Copy) are used as input documents to the CAF.

What is the disposition schedule?

Retire to IRS C-Site one year after year of processing. Destroy after January 2 of the year following the purge year which is identified by the first 2 digits of the SDLN on the POA or TIA. (Job No. NC1-58-85-10, Item 54)

Data Locations

What type of site is this?

System

What is the name of the System?

CI CAF Shared Mailbox

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the System.

Microsoft Outlook Shared Inbox for processing and receiving CAF referrals suspected of being compromised and for dissemination of client/CAF holder/POA information.

What are the incoming connections to this System?

Microsoft Outlook

What type of site is this?

Shared Drive

What is the name of the Shared Drive?

CAF Comp Network Shared Drive

What is the sensitivity of the Shared Drive?

Personally Identifiable Information (PII) including Linkable Data.

Please provide a brief description of the Shared Drive.

Shared Drive to store new CAF reference files

What are the incoming connections to this Shared Drive?

Microsoft 365

What type of site is this?

SharePoint Online (SPO) Collection

What is the name of the SharePoint Online (SPO) Collection?

CAF Tracking SharePoint

What is the sensitivity of the SharePoint Online (SPO) Collection?

Personally Identifiable Information (PII) including Linkable Data

Please provide a brief description of the SharePoint Online (SPO) Collection.

SharePoint location CI CAF Compromise team tracks CAF referrals.

What are the incoming connections to this SharePoint Online (SPO) Collection?

Microsoft 365