Date of Approval: 11/15/2024
Questionnaire Number: 1343

Basic Information/Executive Summary

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

Web Currency and Banking Retrieval System, WebCBRS

Acronym:

WebCBRS

Business Unit

Small Business and Self Employed

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.

Since December 2011 Financial Crimes Enforcement Network (FinCEN) is the data owner. As of December 2012, all external users have been removed. FinCEN is the regulatory agency responsible for the information contained on the Currency Transaction Reports (CTR's) and is the system of record for BSA data. The data comes into WEBCBRS on a daily FTP transmission. The Currency and Banking Retrieval System (WebCBRS) is an on-line database that contains Bank

Secrecy Act (BSA) information. IRS field agents in Small Business Self Employed (SB/SE), Large Business and International (LB&I), and Criminal Investigations Divisions (CID) access the database for research in tax cases, tracking money-laundering activities, investigative leads, intelligence for the tracking of currency flows, corroborating information, and probative evidence. Title 31 BSA data is submitted electronically through the FinCEN's modernized e-filing system, which is the system of record for all BSA data. The FinCEN transmits the BSA data to WebCBRS where it is loaded directly into the WebCBRS database.

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).

Since December 2011 Financial Crimes Enforcement Network (FinCEN) is the data owner. As of December 2012, all external users have been removed. FinCEN is the regulatory agency responsible for the information contained on the Currency Transaction Reports (CTR's) and is the system of record for BSA data. The data comes into WEBCBRS on a daily FTP transmission. The Currency and Banking Retrieval System (WebCBRS) is an on-line database that contains Bank Secrecy Act (BSA) information. IRS field agents in Small Business Self Employed (SB/SE), Large Business and International (LB&I), and Criminal Investigations Divisions (CID) access the database for research in tax cases, tracking money-laundering activities, investigative leads, intelligence for the tracking of currency flows, corroborating information, and probative evidence. Title 31 BSA data is submitted electronically through the FinCEN's modernized e-filing system, which is the system of record for all BSA data. The FinCEN transmits the BSA data to WebCBRS where it is loaded directly into the WebCBRS database.

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

Employer Identification Number

Social Security Number (including masked or last four digits)

Tax ID Number

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

Information by CI for certain money laundering cases - 18 USC

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 personnel administration IRS employees - 5 USC and Executive Order 9397

SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

1.1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

1.2 What is the IRA Initiative Number?

No

1.3 What type of project is this (system, project, application, database, pilot/proof of concept, power platform/visualization tool)?

Application

1.35 Is there a data dictionary for this system?

Yes

1.4 Is this a new system?

No

1.5 Is there a Privacy and Civil Liberties Impact Assessment (PCLIA) for this system?

Yes

1.6 What is the PCLIA number?

6728

1.7 What are the changes and why?

As a result of the ASCA, The PCLIA does not include SORN 34.037 Audit Trail and Security Records, and auditing occurs for the system. The PCLIA does not list Splunk as the downstream system in the audit trail. At a minimum, it was determined that fields for phone numbers, email addresses, dates of birth, and IP addresses were in the data dictionary, but were not listed on the PCLIA. System owners should ensure all PII that is used, collected, received, displayed, stored, maintained, or disseminated is identified in the PCLIA. See IRM 10.5.1.18.13.3 and IRM 10.5.2 for control and PCLIA requirements.

1.8 If the system is on the As-Built-Architecture, what is the ABA ID of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID for each application covered separated by a comma.

210269

1.9 What OneSDLC State is the system in (Allocation, Readiness, Execution)?

Execution

1.95 If this system has a parent system, what is the PCLIA Number of the parent system?

Not applicable

2.1 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? Contact Disclosure to determine if an accounting is required. Enter "Yes" or "No". If Exempt, type "Exempt".

No

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

Compliance Domain (CD) Governance Board

3.1 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?

No

3.2 What is the methodology used and what database is training your AI?

Not applicable

3.3 Does this system use cloud computing?

No

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

Not applicable

3.32 Does the CSP allow auditing?

Not applicable

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

Not applicable

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

Not applicable

3.4 Is there a breach/incident plan on file?

Not applicable

3.5 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

3.6 Does this system interact with the public through a web interface?

No

3.61 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

Not applicable

3.62 Please upload the approved DIRA report using the Attachments button.

Not applicable

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

Not applicable

3.64 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

The information within WebCBRS comes from Treasury/Bank Secrecy databases and files. Those databases, files (and related forms) provide Privacy Act Notice, consent, and due process to individuals. Due process is provided pursuant to 5 USC.

3.65 If information is collected from third-party sources instead of the individual, please explain your decision.

Not applicable

3.7 Describe the business process allowing an individual to access or correct their information.

Not applicable

4.1 Who owns and operates the system (IRS Owned and Operated, IRS Owned and Contractor Operated, Contractor Owned and Operated)?

IRS Owner and Operated

4.2 If a contractor owns or operates the system, does the contractor use subcontractors?

Not applicable

4.3 What PII/SBU data does the subcontractor have access to?

Not applicable

4.5 Identify the roles and their access level to the PII data. For contractors, indicate whether their background investigation is complete or not.

Not applicable

4.51 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”.

More Than 100,000.

4.52 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

4.53 How many records in the system are attributable to members of the public? Enter “Under 5,000”, “5,000 to 10,000”, “More than 10,000” or “Not applicable”.

More than 10,000

4.54 If records are attributable to a category not mentioned above in 4.51 through 4.53, please identify the category and the number of corresponding records to the nearest 10,000. If none, enter "Not Applicable".

Not applicable

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

Access to the data is determined by agency and information supplied in Online Business Entitlement Access Request System (BEARS). BEARS contains rules of behavior for accessing information systems. Both the employee and the employee’s manager login to BEARS. When the employee login to BEARS, they are accountable for his/her misuse of the system. Users of WebCBRS are granted least use access (Read Only). Additionally, system profiles limits or grants access to the various Bank Secrecy Act (BSA) data. All users of WebCBRS are profiled for least access “Read Only”. For example, IRS Revenue Officers, Revenue Agents, and Special Agents have access to all forms.

5.1 Please describe any privacy risks, civil liberties and/or security risks identified for the system that need to be resolved and what is the mitigation plan?

Not applicable

5.11 Is there a Risk Assessment Form and Tool (RAFT) associated with this system on file with your organization or the IRS Risk Office.

No

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

Yes

5.3 Please upload the approved SBU Data Use Questionnaire or Request. If the request has been recertified, please upload the approved recertification form. Select Yes to indicate that you will upload the SBU Data Use form.

Yes

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

Compliance Data Environment (CDE)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Electronic File Transfer Utility (EFTU)

Interface Type

IRS Systems, file, or database

Agency Name

Splunk

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Secure Data Transfer (SDT)

Interface Type

IRS Systems, file, or database

Agency Name

Automated Magnetic Medial Processing System (AMMPS)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Other

Other Transfer Method

Magnetic Media

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 42.031 - Anti-Money Laundering/Bank Secrecy Act and Form 8300

Describe the IRS use and relevance of this SORN.

To administer 26 U.S.C. 6050I and the Bank Secrecy Act.

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 but unclassified information and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy (e.g., gambling, playing computer games, or engaging in illegal activity), or to detect electronic communications sent using IRS systems in violation of IRS security policy.

SORN Number & Name

IRS 46.050 - Automated Information Analysis System

Describe the IRS use and relevance of this SORN.

To maintain, analyze, and process records and information that may identify patterns of financial transactions indicative of criminal and/or civil noncompliance with tax, money laundering, Bank Secrecy Act, and other financial laws and regulations delegated to CI for investigation or enforcement, and that identifies or may identify the individuals connected to such activity. To establish linkages between fraudulent transactions or other activities, and the individuals involved in such actions, that may be used to further investigate such activity and to perfect filters that identify information pertaining to such activity.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Record Control Schedule

What is the GRS/RCS Item Number?

255

What type of Records is this for?

Both (Paper and Electronic)

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

Covers records once created by the Detroit Computing Center responsible for the performance of non-master file data processing operations for the Service, projects for directors of functions at the IRS Headquarters and some bureaus of the Department of the Treasury and other government agencies. Detroit is no longer a Computing Center. This RCS is under review. Detroit recordkeeping activities now at Martinsburg should follow the disposition instructions in this Schedule until further notice.

What is the disposition schedule?

The current year plus three prior years are kept on-site. Documents are retired to the Federal Records Center three years after the end of the processing year and destroyed eleven years after the end of the processing year. Procedures are published in IRS Document 12990 under Records Control Schedule 18, IRM 1.15.18, Item 15. On-Line: The maintenance of similar electronic data in WebCBRS is needed for 20 plus years. WebCBRS is unscheduled and retention requirements will be more specifically defined in the context of a request for disposition authority to the National Archives. The BU/system owner will work with the IRS Records and Information Management (RIM) Program Office to draft the WebCBRS records schedule. The proposed retention for WebCBRS is modeled after data retention approved by NARA for the Title 31 non-Banking Financial Institution Database (Title 31, Job No. DAA-0058-2012-007, approved 2/1/2013). FinCEN is now the Title 31 data system owner. Title 31 data shared with IRS is downloaded to WebCBRS for distribution to other IRS components that need the information for examination and/or investigative purposes.