Date of Approval: 09/24/2025
Questionnaire Number: 2118

Basic Information/Executive Summary

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

View Credit (CRD)

Acronym:

CRD

Business Unit

Information Technology

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.

View Credit (CRD) is an IRS-Owned and operated internal applications that provides authorized IRS personnel with red-only access to taxpayer credit and payment data. CRD retrieves information from Integrated Data Retrieval System (IDRS), Modernized E-File (MeF), and Security and Communications System (SACS), but does not collect, transmit, or modify any PII. Access is restricted to IRS employees; contractors do not have access. The system supports the IRS mission by improving service delivery, enabling timely payment verification, and reducing taxpayer resolution delays.

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).

The PII items are collected from the taxpayer to authenticate them prior to providing them with tax related information. This information represents the least amount of data needed to authenticate the individual, identify possible Identification (ID) theft without any more information on user as possible using existing IRS command codes.

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

Federal Tax Information (FTI)
Name
Other
Social Security Number (including masked or last four digits)
Telephone Numbers

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

Mailing Address, Date of Birth, Protection Personal Identification Numbers (IP PIN)

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

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

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

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?

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?

4243

4.12 What is the previous PCLIA title (system name)?

View Credit (CRD)

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.)

Expiring PCLIA

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

No

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 - CRD has completed development and implementation and is currently in production. All primary functionalities have been deployed, and the system is in operational use while continuing to receive updates and documentation as needed.

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.

Small business/Self-Employed (SBSE) Governance Board

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.

211139

10 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?

No

10.1 You have indicated that you do not have an "accounting of disclosures" process is in place; please indicate a projected completion date or explain the steps taken to develop your accounting of disclosures process. Note: The Office of Disclosure should be contacted to develop this system's accounting of disclosures process.

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?

Yes

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

No

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

View credit does not directly provide individual the opportunity to give consent for information collection, as the data originates from other IRS systems and forms. Notice, consent, and due process are provided through those systems under applicable tax form instructions and pursuant to 5 U.S.C. 552a.

13.3 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.

Individual was not notified because CRD is an internal-facing IRS system that does not collect information directly from individuals. Information processed by CRD originates from pre-existing IRS data systems where appropriate Privacy Act notices have already been provided at the point of initial collection.

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

The information within View Credit comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. View Credit does not directly provide individuals the opportunity to decline from providing information and/or from consenting to uses of the information. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and 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.)

IRS System Administrators - Read only

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.

View Credit (CRD) does not collect PII directly from individuals. The Privacy Act Statement is provided at the point of collection by source systems including IDRS, MeF, and SACS. These systems inform individuals of the authority to collection, how the information is used, and their rights under U.S.C. (552a.) View Credit relies on those systems' Privacy Act Statement.

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".

Not applicable

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

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".

More than 1,000,000

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

Access to the data is determined by the manager based on a user’s position and need-to-know. The manager will request a user to be added. They must submit the request via the Online Business Entitlement Access Request System (BEARS) system to request access to the System.

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.

No

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.

No

26 Describe this system's audit trail in detail. Provide supporting documents.

View Credit uses the Integrated Customer Communication Environment (ICCE) capability to capture audit data and forward the data to an Enterprise Logging System - Security Audit and Analysis System (SAAS). ICCE does not store audit data. Instead, audit records are created in memory and sent to SAAS as “forward and forget”. There is no ability to access the audit information from the application or from the server on which the application runs." as indicated in the previous PCLIA.

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

Integrated Data Retrieval System (IDRS)

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Application to Application (A2A)

Interface Type

Forms

Agency Name

1040 - U.S. Individual Income Tax Return

Incoming/Outgoing

Incoming (Receiving)

Transfer Method

Secured channel via HTTPS

Interface Type
IRS Systems, file, or database
Agency Name
Modernized E-File (MeF)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Secure Data Transfer (SDT)

Interface Type
IRS Systems, file, or database
Agency Name
Security and Communications System (SACS)
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Secure File Transfer Protocol (SFTP)

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.
This SORN covers data retrieved data from the Individual Master File (IMF), which includes tax return data, return transactions, and taxpayer account information. View Credit (CRD) accesses credit-related data maintained in the IMF to support verification, display, and validation of taxpayer credits. The information is used solely to provide internal visibility into claimed credits and to ensure tax administration accuracy.

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
This SORN covers audit trail records, system usage logs, and access monitoring. View Credit (CRD) sends all business layer outbound responses to the IRS Security Audit and Analysis System (SAAS) via AMDAS for audit logging. This supports system accountability, access tracking, and ensures traceability of View Credit queries related to taxpayer records.

SORN Number & Name
IRS 24.046 - Customer Account Data Engine Business Master File

Describe the IRS use and relevance of this SORN.

This SORN supports business return and account information stored in the Business Master File (BMF). While View Credit primarily interfaces with individual data, this SORN is applicable if any business taxpayer or cross-referenced records are included in the validation or display logic. It ensures that any indirect access to BMF data for credit visibility is governed and transparent under Privacy Act requirements.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

Information Systems Security Records

What is the GRS/RCS Item Number?

3.2, Item 030

What type of Records is this for?

Both (Paper and Electronic)

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

System access logs document user login activity, authentications, and access to IRS systems. These records support system security, user monitoring, and audit trail verification. Access logs are transmitted to the WebApps Audit Service and integrated into IRS Cybersecurity's enterprise monitoring tools, including the Security Audit and Analysis System (SAAS) and Splunk, for review and analysis. Records are retained for 6 years after the password is changed or the user separates from access, in accordance with GRS 3.2, item 030. At the conclusion of the retention period, records are erased or purged from the system in accordance with IRM 1.15.6. A control log is maintained containing the media label ID, date and method of destruction, and the signature of the person who destroyed the media.

What is the disposition schedule?

Temporary. Destroy when business use ceases.

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

Information Systems Security Records

What is the GRS/RCS Item Number?

3.2, item 031

What type of Records is this for?

Both (Paper and 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.

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.

Data Locations

What type of site is this?

System

What is the name of the System?

View Credit (CRD)

What is the sensitivity of the System?

Sensitive But Unclassified (SBU)

What is the URL of the item, if applicable?

https://ea.web.irs.gov/aba/SA/ea-panel1_main-application_8042.htm#

Please provide a brief description of the System.

View Credit (CRD) permits a taxpayer who has established a PIN to research a specific payment posted to their account or request a list of the last fifteen payments. This process is currently handled by VoiceBot. The application contains PII, including taxpayer names, SSNs, payment history, and account details. Access is limited to authorized IRS personnel and is monitored through the WebApps Audit Service, with audit and access logs integrated into the Security Audit and Analysis System (SAAS) and Splunk for review and analysis. View Credit (CRD) allows taxpayers to get information about credits posted to their account. The taxpayer is asked to provide the date and amount of a payment, and the application will search and verify the posting of the payment. The taxpayer may also request a list of the last fifteen payments. The application contains Sensitive But Unclassified (SBU) and Personally Identifiable Information (PII), including taxpayer names, SSNs, payment history, and account details. Access is restricted to authorized IRS personnel and monitored through the WebApps Audit Service, with audit and access logs integrated into the Security Audit and Analysis System (SAAS) and Splunk for review and analysis.

What are the incoming connections to this System?

Incoming connections originate from secure IRS systems that provide taxpayer account and payment data for display in View

Credit. These include authenticated service calls and data transfers from the Customer Communications Environment (ICCE) and other IRS master file systems. All incoming connections are encrypted, require multi-factor authentication, and are logged via the WebApps Audit Service, with monitoring in SAAS and Splunk to ensure security and compliance with IRS data handling policies.

What are the outgoing connections from this System?

Outgoing connections from View Credit return requested taxpayer payment and account data to authorized IRS applications and the VoiceBot system for delivery to the taxpayer. These responses are securely transmitted over encrypted channels and adhere to IRS access control policies. All outgoing data flows are logged via the WebApps Audit Service and integrated into SAAS and Splunk for audit and security monitoring.