Date of Approval: 11/07/2025
Questionnaire Number: 2260

Basic Information/Executive Summary

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

(EBR) TINEntry

Acronym:

EBR

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.

TINEntry supports the IRS mission by validating taxpayer identities using Taxpayer Identification Numbers (TIN), Social Security Numbers (SSN), and Employer Identification Numbers (EIN) through the Integrated Customer Communications Environment (ICCE). The system performs lookups through IDRS to determine if callers require Customer Service Representative (CSR) assistance or can proceed with automated self-service options. TINEntry is owned and operated by the Small Business/Self-Employed (SBSE) Division under Information Technology (IT). It is used by IRS employees and CSRs, with limited contractor access for system maintenance under approved security controls. No public users have direct access.

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 system collects the caller's SSN to verify identity and deliver services, such as installment agreements or account-specific inquiries. This data may also be used to rout the caller to the appropriate agent and support self-service applications that assist with tax return completion or other IRS tasks. All data is securely stored, restricted to authorized personnel, and handled according to IRS retention and destruction procedures aligned with NARA (National Archives and Records Administration) and IRM 1.15 policies.

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

Social Security Number (including masked or last four digits)

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 PCLIA a result of a specific initiative or a process improvement?

No

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

Information Technology

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?

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?

7102

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

(EBR) TINEntry

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?

Yes

5.1 Identify the parent system's approved PCLIA number.

A PCLIA Number is not required for Integrated Customer Communications Environment (ICCE).

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

Integrated Customer Communications Environment (ICCE)

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?

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.

211084

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

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?

Yes

13.11 Please upload the approved DIRA report using the Attachments button. Select "Yes" to indicate that you have or will upload the signed DIRA form.

No

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

Individuals can decline from providing information and/or from consenting to uses of information.

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.

Authority to collect the information, whether collection is mandatory or voluntary, purpose, sharing, and effects. TINEntry provides a verbal disclosure during the automated phone process. Callers are informed that the collection of their information is authorized under the Internal Revenue Code and required to verify identity, route calls, and assist with IRS account inquiries. The collection is necessary for accurate taxpayer identification and service delivery.

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

TINEntry does not collect information from third-party sources. All data is provided directly by the caller during the automated phone process.

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

Individuals seeking to access or correct their information may submit a written request in accordance with the Privacy Act of 1974 and IRS regulations. Requests can be made by contacting the IRS Office of Privacy, Governmental Liaison, and Disclosure (PGLD) in writing, following procedures outlined in 26 CFR §601.702 and IRS systems of records notices. TINEntry itself does not directly provide public-facing access or editing capabilities; however, updates or corrections to taxpayer data are managed through authorized IRS channels and validated via official case processing systems.

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.)

TINEntry is managed and operated by IRS personnel. IRS employees with authorized roles may access system data as part of their job duties, consistent with IRS security policies and least-privilege principles. Contractors do not have access to TINEntry or its data.

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.

The Privacy Act Statement is provided verbally at the time of collection when the caller provides their Taxpayer Identification Number (TIN) or Social Security Number (SSN). The statement informs the individual that providing this information is required to verify identity and assist with IRS account-related inquiries.

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 SBU/PII within TINEntry is granted through authenticated user validation and approved BEARS access requests based on role-based permissions and least privilege principles. For taxpayers, access is verified through valid shared secrets that must match existing IDRS/CFOL data to confirm identity before allowing access. For IRS employees, access is managed through BEARS approvals and permissions assigned by the system's Business Owner and System Administrators. Authentication and authorization controls ensure only authorized users can access sensitive data.

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.

The primary privacy and civil liberties risk for TINEntry involve the potential unauthorized access, use, or disclosure of personally identifiable information (PII) collected from taxpayers. These risks are mitigated through strict access controls, audit and tracking logs, encryption of data in transit and at rest, and continuous monitoring. The system follows established procedures under IRC 6103 and the Privacy Act to ensure data is only accessed by authorized users. Supporting documentation, including Audit and Tracking Logs, Risk-Based Decisions (RBDs), POA&Ms, and SAR reports, provide verification of these safeguards and mitigation measures.

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.

TINEntry maintains detailed audit logs to record user activities, including access attempts, data lookups, and changes. These logs support accountability, incident response, and compliance with IRS security standards. Supporting documents including System Security Plan (SSP) and Risk-Based Decision (RBD) documentation.

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
Corporate Files Online
Incoming/Outgoing
Both
Transfer Method
Secure File Transfer Protocol (SFTP)

Interface Type
IRS Systems, file, or database
Agency Name
Integrated Customer Communications Environment (ICCE)
Incoming/Outgoing
Both
Transfer Method
Secure File Transfer Protocol (SFTP)

Interface Type
IRS Systems, file, or database
Agency Name
Integrated Data Retrieval System
Incoming/Outgoing
Both
Transfer Method
Secure File Transfer Protocol (SFTP)

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 00.001 - Correspondence Files and Correspondence Control Files
Describe the IRS use and relevance of this SORN.
TINEntry uses data governed under IRS 00.001 - Correspondence Files and Correspondence Control Files to manage and document taxpayer communications related to authentication, verification, and service requests made through the system. This includes maintaining records of inquiries, responses, and correspondence between the IRS and taxpayers to ensure proper documentation, traceability, and follow-up. These records support transparency, accountability, and the accurate handling of taxpayer interactions, enabling the IRS to deliver timely assistance and maintain a complete audit trail of correspondence activities.

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

TINEntry utilizes data governed under IRS 34.037 - Audit Trail and Security Records System to maintain detailed audit logs and security event tracking for all user interactions within the system. This ensures accountability, transparency, and protection of taxpayer information by recording access, modifications, and queries performed on sensitive data. These audit records support security monitoring, incident investigation, and compliance verification activities, helping the IRS safeguard Personally Identifiable Information (PII) and uphold system integrity in alignment with federal privacy and security standards.

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

TINEntry uses data covered under IRS 24.030 - Customer Account Data Engine Individual Master File (IMF) to verify taxpayer identities and support secure access to IRS services. The system validates caller-provided Taxpayer Identification Numbers (TINs) and Social Security Numbers (SSNs) against existing IRS records to ensure accuracy and authenticity. This process allows the IRS to provide appropriate account-level services, route calls for additional assistance when required and maintain the integrity of taxpayer interactions. The SORN ensures that all records accessed or verified through TINEntry are handled in accordance with the published notice, supporting transparency and lawful use of taxpayer data.

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?

Splunk

What is the sensitivity of the System?

Personally Identifiable Information (PII) including Linkable Data

What is the URL of the item, if applicable?

https://splunk.enterprise.irs.gov

Please provide a brief description of the System.

Splunk is an internal IRS enterprise logging and monitoring platform used to collect, store, and analyze audit and application log data generated by TINEntry. It provides visibility for security, troubleshooting, and audit trail retention purposes. Splunk does not

process taxpayer transactions and is only accessible to authorized IRS personnel.

What are the incoming connections to this System?

TINEntry transmits audit and application event logs to Splunk through secure, encrypted connections within the IRS network. No external or public access is involved. Access to log data is restricted by role-based controls and is used for audit, monitoring, and incident response.

What are the outgoing connections from this System?

There are no outgoing connections from Splunk related to TINEntry. Splunk functions as a one-way log and audit data repository and does not transmit data to any external or downstream systems.