
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. TINV-Enterprise Common Service, TINV-ECS

2. Is this a new system? No

2.a. If no, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If yes, enter the full name, acronym, and milestone of the most recent PCLIA.

TINV-ECS PIA # 1538

Enter the approval date of the most recent PCLIA. 01/04/2016

If yes Indicate which of the following changes occurred to require this update (check all that apply).

- No Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
- No Conversions
- No Anonymous to Non-Anonymous
- No Significant System Management Changes
- No Significant Merging with Another System
- No New Access by IRS employees or Members of the Public
- No Addition of Commercial Data / Sources
- No New Interagency Use
- No Internal Flow or Collection
- Yes Expiring PCLIA

Were there other system changes not listed above? No

3. What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

IT portfolio board, ESGB, Enterprise Services Governance Board.

3.a. Check the current Enterprise Life Cycle (ELC) Milestones (select all that apply).

- No Vision & Strategy/Milestone 0
- No Project Initiation/Milestone 1
- No Domain Architecture/Milestone 2
- No Preliminary Design/Milestone 3
- No Detailed Design/Milestone 4A
- No System Development/Milestone 4B
- No System Deployment/Milestone 5
- Yes Operations & Maintenance (i.e., system is currently operational)

4. Is this a Federal Information Security Management Act (FISMA) reportable system? Yes

A.1 General Business Purpose

5. What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

TINV – Taxpayer Identification Number Validation – This is a common service that allows internal IRS applications to validate Taxpayer Identification numbers for individuals and businesses.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)?

Yes

6.a. If yes, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or tax identification numbers (i.e. last 4 digits, etc.)? Yes

If yes, check all types of tax identification numbers (TIN) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
No Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

No Security background investigations
No Interfaces with external entities that require the SSN
Yes Legal/statutory basis (e.g. where collection is expressly required by statute)
No When there is no reasonable alternative means for meeting business requirements
No Statistical and other research purposes
Yes Delivery of governmental benefits, privileges, and services
No Law enforcement and intelligence purposes
No Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

IRS applications utilize the TIN Validation service to validate both individual SSNs and employer EINs.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN s (or tax identification numbers).

eServices is aware of agency initiatives to reduce SSNs and are willing to participate in the initiatives.

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? Yes

If yes, specify the information.

<u>Selected</u>	<u>PII Element</u>
Yes	Name
No	Mailing address
No	Phone Numbers
No	E-mail Address
No	Date of Birth
No	Place of Birth
No	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
No	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
No	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
No	Employment Information
No	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

6.d. Are there other types of SBU/PII used in the system? No

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

Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
Yes SSN for tax returns and return information is Internal Revenue Code Section 6109
No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No PII for personnel administration is 5 USC
No PII about individuals for Bank Secrecy Act compliance 31 USC
No Information by CI for certain money laundering cases may be 18 USC

6.f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. Explain the detailed business needs and uses for the SBU/PII, and how the SBU/PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

The access to and control of the Personally Identifiable Information (PII) handled by the Common Service is managed by the applications which access the Common Service. User validation and access to TIN-Validation are currently handled by eServices and the Enterprise Service Bus (ESB).

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

The data that TINV-ECS receives is from internal IRS systems which are deemed reliable and the data is validated for accuracy by the system sending the data as described in that system's PCLIA.

C. PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

9. Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information. Yes

If yes, enter the SORN number(s) and the complete the name of the SORN(s).

<u>SORNS Number</u>	<u>SORNS Name</u>
IRS 00.001	Correspondence Files and Correspondence Control Files
IRS 34.037	Audit Trail and Security Records System
IRS 22.062	Electronic Filing Records
IRS 24.030	Customer Account Data Engine Individual Master File

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11.a. If yes, does the system receive SBU/PII from IRS files and databases? Yes

If yes, enter the files and databases.

<u>System Name</u>	<u>Current PCLIA</u>	<u>Approval Date</u>	<u>SA&A?</u>	<u>Authorization Date</u>
TIN Matching Application(eServices)	Yes	04/20/2018	Yes	12/05/2017
Branded Prescription Drug (BPD)	Yes	06/29/2018	No	
Transition Database (XDB)	No		No	
Taxpayer Identification Number Matching - Bulk (TINMB)	Yes	04/20/2018	Yes	12/05/2017
Information Sharing & Reporting - Sharing (ISR-S)	Yes	09/07/2018	No	
Information Returns Processing Validation & Perfection (IRP VAL)	Yes	03/09/2017	No	
Affordable Care Act Information Returns (ACA/AIR)	Yes	10/17/2016	Yes	06/17/2018

11.b. Does the system receive SBU/PII from other federal agency or agencies? No

11.c. Does the system receive SBU/PII from State or local agencies? No

11.d. Does the system receive SBU/PII from other sources? No

11.e. Does the system receive SBU/PII from Taxpayer forms? No

11.f. Does the system receive SBU/PII from Employee forms (such as the I-9)? No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If yes, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

<u>System Name</u>	<u>Current PCLIA</u>	<u>Approval Date</u>	<u>SA&A?</u>	<u>Authorization Date</u>
ACA Information Returns (AIR)	Yes	10/17/2016	Yes	06/17/2018
TIN Matching Application(eServices)	Yes	04/20/2018	Yes	12/05/2017

Identify the authority. IRS Tax Administration.

For what purpose? IRS Tax Administration.

12.b. Does this system disseminate SBU/PII to other Federal agencies? No

12.c. Does this system disseminate SBU/PII to State and local agencies? No

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12.e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No
14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No
15. Does the system use cloud computing? No
16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? Yes

17.a. If yes, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

Notice is provided to individuals by other IRS applications or through forms that interact directly with the taxpayer at the time of collection. Notice, consent and due process are provided pursuant to 5 USC.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18.b. If individuals do not have the opportunity to give consent, why not?

The IRS has the legal right to ask for information per IRC sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for". Their response is mandatory under these sections. Notice, consent and due process are provided pursuant to 5 USC.

19. How does the system or business process ensure due process regarding information access, correction and redress?

Notice is provided to individuals by other IRS applications or through forms that interact directly with the taxpayer at the time of collection. Notice, consent and due process are provided pursuant to 5 USC.

I. INFORMATION PROTECTION

20. Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated) IRS Owned and Operated

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level (Read Only/Read Write/Administrator)</u>
-----------------------	---------------	--

Users	No	
Managers	No	
Sys. Administrators	Yes	Read-Only
Developers	No	

Contractor Employees? No

21.a. How is access to SBU/PII determined and by whom? Access to TINV-ECS is determined by the user's need to know. Only System Admin or production support staff would have the typical access available to any production system through the Online 5081 process.

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? No

22.b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? Yes

23.a. If yes, what date was it completed? 06/28/2018

23.1 Describe in detail the system's audit trail. A complete audit trail of the use of the system is captured and includes every login, logoff, file access and database query. The system monitors for security risks and compliance violations to ensure that the use of the system takes place only for an approved purpose that is within the professional responsibility of each user. TINV-ECS is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a. If yes, was the test plan completed? Yes

24.a.1. If yes, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? DocIT (Web-based document management system)

24.a.2. If yes, were all the Privacy Requirements successfully tested? Yes

24.a.3. If yes, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? eServices continuous monitoring testing is currently being conducted. All documents are being updated.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

- | | |
|------------------------------|-----------------------------|
| 26.a. IRS Employees: | <u>Not Applicable</u> |
| 26.b. Contractors: | <u>Under 5,000</u> |
| 26.c. Members of the Public: | <u>100,000 to 1,000,000</u> |
| 26.d. Other: | <u>No</u> |

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent? No

End of Report
