Date of Approval: February 20, 2019 PIA ID Number: 3692

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Enterprise Telephone Database, ETD-1

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.

Enterprise Telephone Database, ETD-1 PCLIA #1500

Enter the approval date of the most recent PCLIA. 12/08/2015

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. User and Network Services (UNS) 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? No

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.

The Enterprise Telephone Database (ETD-1) is a data warehouse, which stores information from various systems or sources (Aspect Automatic Call Distributors, Cisco, Intelligent Contact Management (ICM), AT&T Telephone Reports, Integrated Customer Contact Environment, Telephone Routing Information System Management Information System (MIS)) regarding IRS telephone service to taxpayers. In addition to being the data repository for telephone MIS, ETD also contains custom-built reports/applications utilizing this telephone data. The ETD system summarizes the data and produces multiple web-based reports used to evaluate the effectiveness of Internal Revenue Service telephone operations to properly evaluate the prior day's telephone performance. In addition to the web-based reports, ETD has a partitioned file share area which contains data from queries which are run against the ETD databases. It allows Joint Operations Center (JOC) and Business Operating Division (BOD) analysts to use the data to analyze call patterns/activity related to their program areas. The primary users are JOC personnel, Wage & Investment and Small Business Self Employed BOD analysts both Compliance and Accounts Management; Tax Exempt Government Entities analysts, and managers at each of the IRS call sites.

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.)? No

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.

Selected	PII Element
No	Name
No	Mailing address
Yes	Phone Numbers
No	E-mail Address
No	Date of Birth
No	Place of Birth
Yes	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? Yes

If yes, select the types of SBU

Selected	**SBU Name**	**SBU Description**
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	Official Use Only (OUO) or Limited Official Use (LOU)	Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.
No	Proprietary data	Business information that does not belong to the IRS
No	Protected Information	Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

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)
No	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
Yes	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 collection and display of taxpayer's Automatic Number Identification (ANI) allows the IRS to understand, interpret and diagnose taxpayer service issues in order to improve quality. This information will identify congestion and demand against IRS toll free products that may subsequently require redesign or additional staffing to reduce the number of dialed attempts required to receive service. Organizations may request this information, but special independent queries must be run against call detail records to cull and produce this information. In addition to the ANI, call detail records includes information about the agent that answered the call (SEID) how and/or why a call was disconnected or abandoned, date/time of the call, original Customer Dial Number, information on call duration, such as talk time, hold time, warp time, queue time, router call key/unique identifier for the call, skill group that handled the call, application the call was sent to (i.e. Refunds, Individual Master File Accounts), which sites were available for queueing the call, language the customer selected, and announcements that played throughout the call.

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

The ETD reports are not driven by SBU/PII data, but by the information pertaining to the telephone call that is contained in the call detail records. There is no validation of SBU or PII data because there is no report created in ETD that contains that type of data. Part of the call record is the customer's telephone number and the SEID of the assistor that handled the call. Telephone data is downloaded from Verizon telephone databases and compiled into a readable report. That data is then compared to prior week and year data along with other analyses to verify accuracy and completeness.

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).

SORNS Number	SORNS Name
24.030	Customer Account Data Engine Individual Master File
24.046	Customer Account Data Engine Business Master File
34.037	Audit Trail and Security Records System
00.001	Correspondence Files and Correspondence Control Files
36.003	General Personnel and Payroll Records

*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.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Aspect Automated Call Distributors	No		No	
Intelligent Contact Manager	No		No	
Unified Contact Center Enterprise	No		No	

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? 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? No

17.b. If no, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.
The only PII collected into the system is the phone number provided in the reports received from Verizon and the employee's SEID from ICM. Neither the phone number nor the SEID information is used in any reports in the system.

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 phone number is captured when the individual calls the IRS Toll Free number and there is not an option for the customer to not provide a phone number. The SEID is needed to determine if a call was answered by an assistor but is not displayed in any of the performance reports.

19. How does the system or business process ensure due process regarding information access, correction and redress?
This system primary function is to provide performance measures on IRS Telephone Operations. Customer phone numbers plays no part in performance reporting.

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

IRS Employees?	**Yes/No**	**Access Level (Read Only/Read Write/ Administrator)**
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Read and Write
Developers	No	

Contractor Employees? Yes

Contractor Employees?	**Yes/No**	**Access Level**	**Background Invest. Level**
Contractor Users	Yes	Read-Only	High
Contractor Managers	Yes	Read-Only	High
Contractor Sys. Admin.	Yes	Read-Only	High
Contractor Developers	Yes	Read-Only	High

21.a. How is access to SBU/PII determined and by whom? Access to the raw data is approved by the project manager based solely upon impact to the system performance. This is the only method the PII in the system can be accessed and is not available to the average user. Access to the information is only granted through the OL5081 application. The ETD SYS ADMIN (Enterprise Telephone Database) system utilizes the standard IRS on–Line access application to document approvals for access. Data access is granted on a need-to-know basis. A potential user must submit a request for access to their local management for approval. Users are not permitted access without a signed form from an authorized management official. Specific permissions (Read, Write, Modify, Delete, and/or Print) are defined on the form and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to.

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? Yes

22.a. If yes, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and title.

The IRS Identity and Records Protection Office is currently developing a new section under Records Control Schedule specific to ETD and electronic records retention.

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? No

23.c. If no, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements? Yes

23.1 Describe in detail the system's audit trail. No audit trail, for users of the ETD-1 website, has been implemented because there was no benefit in tracking detailed user information when the data available to the user in EDT-1 could not be used to identify an individual and all users were behind the IRS firewall. Access to the database is controlled by the OL5081 process. In addition, any change to production coming out of the development/test environments are submitted via the transmittal process. The transmittal contains the developer's name and phone number. Further, only the System Analysts (the specific IRS Information Technology employees) have write access. This small group of IRS employees as well as all other users of the database would have to use Microsoft Sequel (SQL) queries to see EDT-1 data and the SQL logs are the audit trail for those actions. Their access is also obtained through the OL5081 application. SQL logging is unavailable to us at this time due to space limitations on the production server. To ensure the auditability of the ETD-1 system, a custom audit trace has been installed as part of IRS database hardening. Audit logs are written to a file and stored on the P: Drive for all ETD-1 SQL servers. All events are audited. In addition to the custom audit trace, the Default Trace is enabled for all ETD-1 SQL servers, which captures database events, errors and warnings, full-text events, object events, security audit events, configuration changes and server memory events. ETD-1 web server (IIS) session events/requests are tracked in a separate log for each website instance, e.g., ETD, Organization Function and Program Codes, etc. on all ETD-1 IIS servers.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24.b. If no, please explain why. All monitoring and evaluating activities are done by the ETD-1 programs that manage the ETD-1.

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:	Under 50,000
26.b. Contractors:	Not Applicable
26.c. Members of the Public:	More than 1,000,000
26.d. Other:	No

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? Yes

31.a. 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. Yes

End of Report