Date of Approval: October 12, 2018 PIA ID Number: **3714**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Automated Collection System, ACS

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.

Automated Collection System, ACS, PIA # 1588

Enter the approval **date** of the most recent PCLIA. 12/18/2015

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.

ACS reports to the AD Compliance 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
Yes 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.
The purpose of the Automated Collection System (ACS) is to collect delinquent taxes and returns through the use of enforcement tools when appropriate. Customer Service Representatives (CSR) use ACS case management abilities to contact taxpayers, review their histories, and issue notices, liens, and/ or levies to resolve the cases. Taxpayer contact is accomplished through incoming and outgoing telephone calls via Automated call distributor (ACD) and through correspondence to taxpayers and third parties. The benefit to the IRS is collection of revenue. The information is used to levy taxpayer wages and/or accounts and file liens to protect the government's interest.

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)
Yes	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)
Yes	When there is no reasonable alternative means for meeting business requirements
No	Statistical and other research purposes
No	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.

They are approved Treasury uses of the SSNs.

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

ACS will use an Alternative identifier, the ACS case reference number. The SSN cannot be completely removed from ACS until there is an Enterprise wide change. ACS requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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
Yes	Name
Yes	Mailing address
Yes	Phone Numbers
No	E-mail Address
Yes	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
Yes	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.
Yes	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
Yes	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)
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.

Taxpayer: Taxpayer information available on ACS relates to a Taxpayer Delinquent Account (TDA) or Taxpayer Delinquency Investigation (TDI). Taxpayer Name Taxpayer Address Telephone Number Taxpayer Identification Number (TIN) Date of Birth (DOB) Adjusted Gross Income (AGI). The SBU/PII (SSN/TIN and address) is used to identify taxpayers when issuing notices including levies and liens and answering incoming telephone calls. This information as well as tax account information is also necessary to ensure issuance to and collection from the correct taxpayer and to ensure the accurate tax amount is collected and the proper returns are requested and secured. Employee: Employee information is stored on the system for the purpose of assigning taxpayer cases, controlling workload, and generating documents and correspondence - Employee name, Employee number, Office location, Work telephone number, Title, Type of access & Team Function/Unit.

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

ACS has validity checks built into the automated system. Real-time error and batch errors identify data entry errors by the Collection Representatives (CR). Validity checks are performed on the data, the action requested, and access to the system. The data validity and action requested validity is performed while the operator is using the system, and an error message is displayed which will validate the data entered or action requested. An employee may receive an error message because they modified a field incorrectly or requested an action that is not allowed. The error message will be displayed on the screen, and the operator must decipher the message and correct the error. Until the error is resolved the operator is not able to leave the screen. No data can be saved until all edits have been performed successfully and an operator has corrected the problems.

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
IRS 26.019	Taxpayer Delinquent Accounts Files
IRS 34.037	Audit Trail and Security Records System

*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
Computer Files On Line (CFOL)	Yes	09/19/2016	No	
Inventory Delivery System (IDS)	Yes	12/05/2016	Yes	09/12/2016
Integrated Data Retrieval System (IDRS)	Yes	10/01/2018	Yes	10/14/2018

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? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Accurint	n/a research tool used by CSRs	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? 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?
The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number. The information is used for the purposes of completing, correcting, or processing a return, figuring tax, and collecting tax, interest and penalties.

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 legal right to ask for information is Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. These sections state that individuals must file a return or statement with IRS for any tax for which they are liable, and response is mandatory.

19. How does the system or business process ensure due process regarding information access, correction and redress?
Publication 1 "Your Rights as a Taxpayer" explains the rights of the taxpayer, which includes the right to challenge the IRS' position and be heard; and the right to appeal an IRS decision in an independent forum. Additionally, as ACS is a system to collect delinquent taxes, collection appeal rights are explained in detail in Publication 1660, Collection Appeal Rights.

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 and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Read and Write
Developers	Yes	Read-Only

Contractor Employees? Yes

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

21.a. How is access to SBU/PII determined and by whom? An ACS Collections Representative (CR) has access to specific cases via TIN or based on their inventory. Access is granted based on the duties of the employee, and only on a need-to-know basis. Online 5081 is required for employees who need to have access to the ACS system as a part of their official duties. By signing this form, employees indicate their understanding and agreement to abide by the rules of behavior for accessing sensitive taxpayer data. The Online 5081 ensures that the user is accountable for any misuse of the system. The employee's manager approves the request to access the system which includes the level of access.

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

I.2 SA&A OR ASCA

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

23.b. If **in process**, when is the anticipated date of the SA&A or ASCA completion? 11/20/2018

23.1. Describe in detail the system's audit trail. The following data elements are collected in the ACS audit trail: Date and time of event Unique identifier (e.g., employee number and Resource Access Control Facility (RACF) Identification (ID) Type of event Subject of the event (e.g., the user, file, or other resource affected) Action taken on that subject Outcome status (success or failure) Date and time of input. ACS 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**, 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)? Test results are stored in TFIMS (Treasury FISMA Inventory 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? Continuous Monitoring (eCM) (now called Annual Security Control Assessment (ASCA)) occurs annually to ensure that controls remain in place to properly safeguard PII.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? Yes

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request? Yes

If **yes,** provide the date the permission was granted. 02/27/2012

25.b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

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

26.a. IRS Employees:	Not Applicable
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