

Date of Approval: January 04, 2024

PIA ID Number: 8513

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Automated Collection System, ACS

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym, and milestone of the most recent PCLIA?

Automated Collection System, ACS, PIA # 6480

What is the approval date of the most recent PCLIA?

10/1/2021

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Expiring PCLIA

Were there other system changes not listed above?

Yes

What were those changes?

The PCLIA does not document the dissemination of PII to the downstream audit logging system. We needed to add ACS audit logs are currently being sent to SPLUNK via EFTU in section 23.1.

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

AD Compliance Governance Board.

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

Operations & Maintenance (i.e. system is currently operational)

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

Yes

GENERAL BUSINESS PURPOSE

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.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

*Legal/statutory basis (e.g. where collection is expressly required by statute)
When there is no reasonable alternative means for meeting business requirements*

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

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.

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

Yes

Specify the PII Elements:

*Name
Mailing address
Phone Numbers
E-mail Address
Date of Birth
Standard Employee Identifier (SEID)
Tax Account Information
Centralized Authorization File (CAF)*

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List (SBUList):

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

Procurement sensitive data - Contract proposals, bids, etc.

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.

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.

Are there other types of SBU/PII used in the system?

No

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

BUSINESS NEEDS AND ACCURACY

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.

How is the SBU/PII verified for accuracy, timeliness, and completion?

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.

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.

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

Identify the Privacy Act SORN(s) that cover these records.

Treasury/IRS 26.019 Taxpayer Delinquent Account Files

Treasury/IRS 34.037 Audit Trail and Security Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

For Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Inventory Delivery System (IDS)

Current PCLIA: Yes

Approval Date: 8/19/2022

SA&A: No

System Name: Integrated Data Retrieval System (IDRS)

Current PCLIA: Yes

Approval Date: 10/26/2021

SA&A: Yes

ATO/IATO Date: 9/21/2023

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

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: Accurint

Transmission Method: Research Tools used by CSRs

ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

No

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

No

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.

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.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Read Write

Developers: Read Only

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. A Business Entitlement Access Request System (BEARS) request 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. BEARS 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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

RCS 28, Items 95-144 i, Part V - Automated Collection System (ACS) records. (Items 95-144)

SA&A OR ECM-R

Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)?

Yes

What date was it completed?

10/31/2023

Describe 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. ACS audit logs are currently being sent to SPLUNK via EFTU.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

Test results are stored in Doc-it under the name System Test Plan (STP).

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress 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.

SBU DATA USE

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

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

2/12/2021

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Not Applicable

Contractors: Not Applicable

Members of the Public: More than 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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

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