

Date of Approval: **June 28, 2023**

PIA ID Number: **7953**

SYSTEM DESCRIPTION

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

AIMS Centralized Information System, ACIS

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?

AIMS - Centralized Information System (A-CIS) PCLIA #6489

What is the approval date of the most recent PCLIA?

10/20/2021

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Were there other system changes not listed above?

Yes

What were those changes?

We now use Business Entitlement Access Request System (BEARS) as an incoming PII interface and Splunk as a Dissemination of PII.

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

Small Business/Self-Employed (SB/SE) 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 AIMS Centralized Information System (ACIS) is an Internal Revenue Service (IRS) system that allows IRS employees to track the status of non-examined, open, and closed IRS audits recorded in Audit Information Management System (AIMS) Related Reports (ARR) and Summary Examination Time Transmission System (SETTS). The application was developed as a monitoring and reporting tool used by IRS analysts to perform detailed analysis to monitor and report on non-examined, open, and closed tax return audits including hours and days to exam the return; IRS organization examining the return; and type of return (like Individual Master File (IMF), Corporate, Employment Tax, 1040 Return with Schedule C form, Offshore Issue, State Tax Refund Issue). Analysis of ACIS data allows the IRS to effectively plan for current and future examinations.

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:

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

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

The Office of Management and Budget CIRCULAR NO. A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The ACIS system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

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

The system requires the use of SSN's 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.

Employer Identification Number

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
Standard Employee Identifier (SEID)
Internet Protocol Address (IP Address)
Tax Account Information

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:

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.

Criminal Investigation Information - Information concerning IRS criminal investigations or the agents conducting the investigations.

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

Yes

Describe the other types of SBU/PII that are applicable to this system.

Tax examination information like IRS employee geographic location; reasons the return was selected for examination; and certain information from tax return like amount of claim, tax year, and business assets are in the system.

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

Has the authority been verified with the system owner?

Yes

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.

ACIS provides IRS analysts the ability to monitor and report on the examination process, open & closed audits, and non-examined returns, at a high level down to an individual tax return. The use of SSNs by the system is needed to uniquely identify a taxpayer's record because no other identifier can be used to uniquely identify a taxpayer. ACIS users are only given access to the information they need to perform their duties. The SBU/PII collected is limited to what is relevant and necessary for tax administration and conducting a proper tax compliance examination. ACIS sends Streaming Data Monitoring Tool only the required audit events and required fields to meet IRS audit requirements.

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

The data is validated on the AIMS system from which it is extracted using consistency checks and record counts. The data is deemed reliable, and the data is validated for accuracy by the system sending the data as described in that system's PCLIA. ACIS and examination staff also review the data and check record counts. If an ACIS staffer discovers a possible error, they communicate with staffers in Examination and the AIMS organization for them to research and resolve the possible error. If there is a substantial error, an ACIS staffer notifies ACIS users.

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.

IRS 42.008 Audit Information Management System

IRS 34.037 Audit Trail and Security Records

IRS 42.001 Examination Administrative Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

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: FOC CDM Phase 2 BEARS (Continuous Diagnostics)

Current PCLIA: Yes

Approval Date: 8/25/2021

SA&A: Yes

ATO/IATO Date: 1/27/2021

System Name: Active Directory (GSS-17)

Current PCLIA: Yes

Approval Date: 8/18/2021

SA&A: Yes

ATO/IATO Date: 3/19/2023

System Name: AIMS Related Reports

Current PCLIA: Yes

Approval Date: 3/14/2022

SA&A: Yes

ATO/IATO Date: 12/9/2022

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?

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?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Streaming Data Monitoring Tool

Current PCLIA: Yes

Approval Date: 12/15/2021

SA&A: Yes

ATO/IATO Date: 4/12/2023

System Name: Business Performance Management System

Current PCLIA: Yes

Approval Date: 8/5/2022

SA&A: Yes

ATO/IATO Date: 2/3/2014

System Name: LB&I Workload Identification System

Current PCLIA: Yes

Approval Date: 9/22/2021

SA&A: Yes

ATO/IATO Date: 4/10/2020

System Name: Excise Files Information Reporting System

Current PCLIA: Yes

Approval Date: 9/22/2022

SA&A: Yes

ATO/IATO Date: 5/4/2023

System Name: Issues Based Management Information System - Reporting

Current PCLIA: Yes

Approval Date: 2/13/2023

SA&A: Yes

ATO/IATO Date: 3/23/2023

System Name: Data Capture System (DCS)

Current PCLIA: Yes

Approval Date: 8/18/2022

SA&A: Yes

ATO/IATO Date: 10/24/2022

Identify the authority.

Authority and purpose is pursuant to section 6103(h)(1) of the IRC. IRC 6103(h)(1) provides for disclosure of returns and return information to officers and employees of the Department of the Treasury (including IRS) whose official duties require access for tax administration.

For what purpose?

Access is needed for tax administration.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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 in tax return instructions. When a return is selected for examination, the taxpayer is sent Notice 609, Privacy Act Notice, Pub 3498, The Examination Process, Pub 5, Your Appeals Rights and How to Prepare a Protest Publication 4227, Overview of the Appeals Process.

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

No

Why not?

Information is collected from returns filed, procedural fields, and examination results. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions.

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

The ACIS Database does not make determinations. All determinations are completed through the Examination process with no direct correlation to the ACIS system. IRS policy allows affected parties the opportunity to clarify or dispute negative determinations per the examination appeals.

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 Only
Managers: Read Only
System Administrators: Administrator
Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Only

How is access to SBU/PII determined and by whom?

ACIS relies on the General Support System (GSS) common controls associated with the IRS Enterprise Active Directory (AD) domain structure to uniquely identify and verify the identity of each user. A Business Entitlement Access Request System (BEARS) request is required of IRS users requesting access to ACIS and must be signed by an immediate manager, the respective Business Unit, the ACIS Access Approval, ACIS Application Manager, and then by Enterprise LAN Account Administration group, who adds the new user's account into the system. The BEARS process ensures that the user identifier is issued to the intended party and that user identifiers are archived. For access to ACIS, users must first successfully authenticate to their respective GSS infrastructure utilizing their IRS account provided through the BEARS process. Once successfully authenticated, ACIS users are transparently given the proper permissions, through domain group policy, to access the ACIS application subset of data they are authorized to view to run queries and generate reports.

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.

ACIS is a non-recordkeeping tracking and analysis tool. All records are generated and maintained in the Audit Information Management System (AIMS) Related Reports (ARR) and Summary Examination Time Transmission System (SETTS) will be managed according to requirements under IRM 1.15.1 and 1.15.6 and will be destroyed using IRS Records Control Schedule (RCS) 23 for Tax Administration-Examination; and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

SA&A OR ASCA

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

Yes

What date was it completed?

10/27/2022

Describe the system's audit trail.

All users logon to the ACIS application using Active Directory. Thus, the logon information is captured in the GSS-17 and GSS-30 audit trail. Users query the data tables on the ACIS Sequel Server (SQL) server, where each query is captured in the ACIS audit logs. The audit trails produced by ACIS maintain a record of system activity and are created within the SQL Server Audit Trails on the server. The logs are picked up and stored offsite as required by the Internal Revenue Manual by another Information Technology (IT) organization. Required audit events are sent to Streaming Data Monitoring Tool daily.

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)?

All software is tested by IT, so they have their test results. The ACIS team tests to make sure the application works as needed and permission to data is limited to least privileges. The team's test documentation is stored on the ACIS Technical SharePoint site.

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?

Permissions are tested each month to verify they are correct. Least privileges are considered when each ACIS user is approved for access to the application. Record retention is based on business requirements, "Delete when no longer needed". All IRS employees take privacy awareness training.

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.

10/19/2021

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?

No