Date of Approval: November 20, 2018 PIA ID Number: **3672**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. AIMS – Centralized Information System, A-CIS

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.

AIMS – Centralized Information System (A-CIS) PCLIA #1448

Enter the approval **date** of the most recent PCLIA. 10/09/2015

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.

Small Business/Self-Employed (SB/SE) 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.
The AIMS – Centralized Information System (A-CIS) 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 A-CIS data allows the IRS to effectively plan for current and future examinations.

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

The Office of Management and Budget Memorandum M-17-12 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 A-CIS 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). None

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
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
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
No	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
Yes	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? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system.

Tax examination information like IRS employee ID number and 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.

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.

A-CIS 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. A-CIS 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.

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

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. A-CIS and examination staffers also review the data and check record counts. If an A-CIS 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 A-CIS staffer notifies A-CIS users.

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 42.008	Audit Information Management System
IRS 34.037	IRS Audit Trail and Security Records System
IRS 42.001	Examination Administrative Files

*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
AIMS Related Reports	Yes	08/30/2018	Yes	05/07/2012

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.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Business Performance Management System	Yes	11/15/2016	Yes	01/15/2014
LB&I Workload Identification System	Yes	03/05/2018	Yes	02/05/2013
Excise Files Information Reporting System	Yes	01/13/2017	Yes	03/29/2018
Issues Based Management Information System – Reporting	Yes	12/22/2016	Yes	12/08/2017
Data Capture System (DCS)	Yes	03/16/2016	Yes	08/06/2017

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.

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?
The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. See Treasury Directive Publication (TDP) 25-07 Section 4.4 for further details on notice. 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.

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?
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.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The A-CIS Database does NOT make determinations. All determinations are completed through the Examination process with no direct correlation to the A-CIS system. IRS policy allows affected parties the opportunity to clarify or dispute negative determinations per the examination appeals.

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	Administrator
Developers	Yes	Read and Write

Contractor Employees? No

21.a. How is access to SBU/PII determined and by whom? A-CIS 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. An OnLine 5081 (OL5081) request is required of IRS users requesting access to A-CIS and must be signed by an immediate manager, the respective Business Unit, the A-CIS Access Approval, A-CIS Application Manager, and then by Enterprise LAN Account Administration group, who adds the new user's account into the system. The OL5081 process ensures that the user identifier is issued to the intended party and that user identifiers are archived. For access to A-CIS, users must first successfully authenticate to their respective campus domain GSS infrastructure utilizing their IRS account provided through the OL5081 process. Once successfully authenticated to the campus domain, A-CIS users are transparently given the proper permissions, through domain group policy, to access the A-CIS application databases to run queries and generate reports.

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.

A-CIS 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.

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? 11/01/2017

23.1. Describe in detail the system's audit trail. All users logon to the A-CIS application using AD. Thus, the logon information is captured in the GSS-17 audit trail. Users query the data tables on the A-CIS Sequel Server (SQL) server, where each query is captured in the A-CIS audit logs. The audit trails produced by A-CIS 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.

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)? All software is tested by IT so they have their test results. The A-CIS 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 A-CIS Technical SharePoint site.

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

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? Permissions are tested each month to verify they are correct. Least privileges are considered when each A-CIS 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.

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. 04/07/2016

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? No

End of Report