

Date of Approval: October 9, 2015

PIA ID Number: **1448**

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

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

AIMS – Computer Information System A-CIS PIA 9 16 2009

Next, enter the **date** of the most recent PIA. 8/21/2012

Indicate which of the following changes occurred to require this update (check all that apply).

No Addition of PII
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

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) 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

6a. 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 who the SSN (or tax identification number) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes Social Security Number (SSN)
Yes Employer Identification Number (EIN)
No Individual Taxpayer Identification Number (ITIN)
No Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
No Practitioner Tax Identification Number (PTIN)

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

The Office of Management and Budget memorandum M-07-16 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. A-CIS 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.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	No
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No

No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
Yes	Tax Account Information	Yes	Yes	No

6c. 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

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
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.
----	------------------------------------	---

6d. 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.

6e. 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

6f. 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? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

The data is validated on the AIMS and Summary Examination Time Transmission System (SETTS) 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 Privacy & Civil Liberties Impact Assessment (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 exam 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

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number

SORNS Name

Treasury/IRS 42.008 Audit Information Management System

Treasury/IRS 34.037 IRS Audit Trail and Security Records System

Treasury/IRS 42.001 Exam Administrative Files

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. N/A

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
AIMS Related Reports	Yes	05/12/2015	Yes	05/22/2012

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? No

11e. Does the system receive SBU/PII from **Taxpayer** forms? No

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. 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.

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA & A?</u>	<u>Authorization Date</u>
Business Performance Management System	Yes	11/12/2013	No	
LB&I Workload Identification System	Yes	04/03/2012	No	
Excise Files Information Reporting System	Yes	02/13/2014	Yes	05/20/2015
Issues Based Management Information System – Reporting	Yes	01/10/2014	No	05/20/2015
Planning Analysis Inventory & Research	No	01/10/2014	No	05/20/2015

Identify the authority and for what purpose? Authority and purpose is pursuant to section 6103(h)(1) of the Internal Revenue Code (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. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

12b. Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. 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, cloud, global position system (GPS), biometrics, 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/is notice provided to the individual prior to collection of information? Yes

17a. 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. 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

18b. If 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.

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 process.

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

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level(Read Only/Read Write/Administrator)</u>
Users	Yes	Read-Only
Managers	Yes	Read-Only
Sys. Administrators	Yes	Read-Only
Developers	Yes	Read And Write

Contractor Employees? Yes

<u>Contractor Employees?</u>	<u>Yes/No</u>	<u>Access Level</u>	<u>Background Invest.</u>
Contractor Users	No		
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Read and Write	Moderate
Contractor Developers	No		

21a. 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 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.

- 21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ?
Not Applicable

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

- 22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

A-CIS is unscheduled. Application staffers are working with the IRS Records and Information Management (RIM) Office to draft and seek National Archives approval of A-CIS data retention instructions. We retain records as needed by Exam.

I.2 SA&A OR ECM-R

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

- 23a. If **yes**, what date was it completed? 9/2/2015

23.1 Describe in detail the system's audit trail. All users log-in to the A-CIS application using Active Directory. Thus, the log-in information is captured in the GSS-17 audit trail. Users query the data tables on the A-CIS 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 C-2 Audit Trails on the SQL Server, hosted on the GSS-30 server. The logs are picked up and stored offsite as required by the Internal Revenue Manual (IRM) by another Information Technology (IT) organization.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

- 24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process**, 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?

All software is tested by IT. A-CIS does not use any "specialty" software. Application developers test to make sure the application works as needed and permission to data is limited to least privileges.

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? All software is tested by Information Technology so they will have the results.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

If **yes**, please describe the outstanding issues.

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. 4/2/2014

25b. If **yes**, was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy? Yes

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: More than 1,000,000
26d. 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 9/11 Commission Recommendations 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

N. ACCOUNTING OF DISCLOSURES

30. 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
