NOTE: The following reflects the information entered in the PIAMS website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: April 24, 2015 PIA ID Number: **1045**

1. What type of system is this? New

1a. Is this a Federal Information Security Management Act (FISMA) reportable system? No

2. Full System Name, Acronym, and Release/Milestone (if appropriate):

ATLAS, NA

2a. Has the name of the system changed? No

If yes, please state the previous system name, acronym, and release/milestone (if appropriate):

3. Identify how many individuals the system contains information on

Number of Employees:	Under 50,000
Number of Contractors:	Not Applicable
Members of the Public:	Over 1,000,000

4. Responsible Parties:

NA

5. General Business Purpose of System

This is used for Criminal Investigation Case Management. Allowing Management, Special Agents, and other CI Employees to manage criminal investigations as well as de-conflicting potential entities involved in other investigations. Atlas is a system that is going to be used to be a repository for case data, but also cross checks (or de-conflicts) that case data, to see if there is another case that has relevant information to the first case. If this does occur, it contacts the two agents working the case This system is designed to hold case data, which would mean anything that is related to the case. That would include any and all forms the IRS uses.

6. Has a PIA for this system, application, or database been submitted previously to the Office of Privacy Compliance? (*If you do not know, please contact* *Privacy *and request a search*) Yes

6a. If **Yes**, please indicate the date the latest PIA was approved: 4/30/2013 12:00:00 AM

6b. If **Yes**, please indicate which of the following changes occurred to require this update.

- System Change (1 or more of the 9 examples listed in OMB 03-22 applies) (refer to PIA Training Reference Guide for the list of system changes) No
- System is undergoing Security Assessment and Authorization No

6c. State any changes that have occurred to the system since the last PIA

Application changed its name

7. If this system has an Exhibit 53 or Exhibit 300 please provide the Unique Project Identifier (UPI) number (XXX-XX-XX-XX-XX-XXXX-XX). Otherwise, enter the word 'none' or 'NA'. none

B. DATA CATEGORIZATION

Authority: OMB M 03-22 & PVR #23- PII Management

8. Does this system collect, display, store, maintain or disseminate Personally Identifiable Information (PII)? Yes

9. Indicate the category that best describes the source that provides or originates the PII collected, displayed, stored, maintained or disseminated by this system. Most common categories follow:

Taxpayers/Public/Tax Systems	Yes	
Employees/Personnel/HR Systems	Yes	
Other	Yes	*Other Source:* Any name or business found through an investigation.

10. Indicate all of the types of PII collected, displayed, stored, maintained or disseminated by this system. Then state if the PII collected is on the Public and/or Employees. Most common fields follow:

TYPE OF PII	Collected?	On Public?	On IRS Employees or Contractors?
Name	Yes	Yes	Yes
Social Security Number (SSN)	Yes	Yes	Yes
Tax Payer ID Number (TIN)	Yes	Yes	Yes
Address	Yes	Yes	Yes
Date of Birth	Yes	Yes	Yes

Additional Types of PII: Yes

PII Name	On Public?	On Employee?
Any and all elements that are related to a case.	Yes	Yes

10a. What is the business purpose for collecting and using the SSN ?

Any PII related to an open and working case to include PII related to subjects, victims, informants and any other source related to case information.

If you answered **Yes** to Social Security Number (SSN) in question 10, answer **10b**, **10c**, and **10d**.

10b. Cite the authority that allows this system to contain SSN's? (e.g. specific regulations, statutes, etc.)

The use of SSN's as a specific, unique and verifiable identifier as part of an on-going investigation ensures clear and accurate identification of the entities involved in an investigation.

10c. What alternative solution to the use of the SSN has/or will be applied to this system? (e.g. masking, truncation, alternative identifier)

There is no other alternative available that allows accurate identification of all entities.

10d. Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of Social Security Numbers on this system?

There is no plan to eliminate the use of SSN's as the key identifiers in investigation as they are universally accepted by the court systems, defense attorneys and prosecutors

Describe the PII available in the system referred to in question 10 above.
Anything related to an open and working case.

11. Describe in detail the system's audit trail. State what data elements and fields are collected. Include employee log-in information. If the system does not have audit capabilities, explain why an audit trail is not needed.

Audit trails are generated at the operating system level for login and at the database level per IRM 10.8.3. Login information includes username, date and time of login, logout, and failed logins

11a. Does the audit trail contain the audit trail elements as required in current IRM 10.8.3 *Audit Logging Security Standards*? Yes

12. What are the sources of the PII in the system? Please indicate specific sources:

a. IRS files and databases: Yes

If **Yes**, the system(s) are listed below:

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
CIMIS	Yes	07/10/2013	No	

b. Other federal agency or agencies: Yes

If **Yes**, please list the agency (or agencies) below:

To include but not limited to; FBI, DEA, USSS, and Any relevant to the case. The Atlas application does not pull from any databases or sources other than CIMIS.

c. State and local agency or agencies: Yes

If **Yes**, please list the agency (or agencies) below:

Same as b. above. For example: To include but not limited to; informants, witnesses, victims, subjects, and business entities such as banks, and brokerages. Any relevant to the case.

d. Third party sources: Yes

If yes, the third party sources that were used are:

Same as above. For example: To include but not limited to; informants, witnesses, victims, subjects, and business entities such as banks, and brokerages. Any relevant to the case.

e. Taxpayers (such as the 1040): Yes

f. Employees (such as the I-9): Yes

g. Other: Yes If **Yes***, specify*: Any relevant to the case.

C. PURPOSE OF COLLECTION

Authorities: OMB M 03-22 & Internal Revenue Manual (IRM) 10.8.8, IT Security, Live Data Protection Policy & PVR #16, Acceptable Use

13. What is the business need for the collection of PII in this system? Be specific.

To find investigations that are related to each other. Officer Safety, limiting and controlling contact in investigations. To have a uniformed collection process for agents to manage and maintain case information.

D. PII USAGE

Authority: OMB M 03-22 & PVR #16, Acceptable Use

14. What is the specific use(s) of the PII?

To conduct tax administration	Yes	
To provide taxpayer services	No	
To collect demographic data	No	
For employee purposes	No	
		If other, what is the use?
Other:	Yes	To ensure accurate identification of all parties involved in investigations.

E. INFORMATION DISSEMINATION

Authority: OMB M 03-22 & PVR #14- Privacy Notice and #19- Authorizations

15. Will the information be shared outside the IRS? (for purposes such as computer matching, statistical purposes, etc.) Yes

15a. If yes, with whom will the information be shared? The specific parties are listed below:

	Yes/No	Who?	ISA OR MOU**?
Other federal agency (-ies)	Yes	Any agency to work federal violations.	Yes
State and local agency (-ies)	Yes	Any agency to work federal violations.	Yes
Third party sources	Yes	Defense attorneys involved in that criminal investigation. Release of information would be related to the discovery process involved in a Criminal Investigation.	No
Other:	No		

** Inter-agency agreement (ISA) or Memorandum of Understanding (MOU)

16. Does this system host a website for purposes of interacting with the public? No

17. Does the website use any means to track visitors' activity on the Internet?
If yes, please indicate means:

	YES/NO	**AUTHORITY**
Persistent Cookies		
Web Beacons		
Session Cookies		
		If other, specify:
Other:		

F. INDIVIDUAL CONSENT

Authority: OMB M 03-22 & PVR #15- Consent and #18- Individual Rights

18. Do individuals have the opportunity to decline to provide information or to consent to particular uses of the information? Not Applicable

19. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action? Yes

19a. If **Yes**, how does the system ensure “due process”?

Atlas stores information related to criminal investigations. That information is used in the judicial system which strictly adheres to procedures and processes designed to ensure due process.

20. Did any of the PII provided to this system originate from any IRS issued forms? Yes

20a. If **Yes**, please provide the corresponding form(s) number and name of the form.

ID	Form Number	Form Name
5106	1040	Individual Tax Return
5107	1040ez	Individual Tax Return
5108	W-4	Employee's Withholding
5109	1099-g	Governent payments
5110	1099-misc	Miscellaneous Income

G. INFORMATION PROTECTIONS

Authority: OMB M 03-22 & PVR #9- Privacy as Part of the Development Life Cycle, #11- Privacy Assurance, #12- Privacy Education and Training, #17- PII Data Quality, #20- Safeguards and #22- Security Measures

21. Identify the owner and operator of the system: IRS Owned and Operated

21a. If Contractor operated, has the business unit provided appropriate notification to execute the annual security review of the contractors, when required?

22. The following people have use of the system with the level of access specified:

	Yes/No	Access Level
IRS Employees:	Yes	
Users		Read Write
Managers		No Access
System Administrators		Read Only
Developers		Read Only
Contractors:	No	
Contractor Users		
Contractor System Administrators		
Contractor Developers		
Other:	No	

If you answered yes to contractors, please answer **22a.** *(All contractor/contractor employees must hold at minimum, a "Moderate Risk" Background Investigation if they have access to IRS owned SBU/PII data.)*

22a. If the contractors or contractor employees act as System Administrators or have “Root Access”, does that person hold a properly adjudicated “High Level”background investigation?

23. How is access to the PII determined and by whom?

Access by the case agent is authorized when assigned the investigation. Further access is delegated to other agents assigned to support the investigation. Participation in the investigation is the basis for determining “the need to know”.

24. How will each data element of SBU/PII be verified for accuracy, timeliness, and completeness?

Up to the agent working case to perform the due diligence to ensure accurate identifiers are used when the agent is establishing an identity. Timeliness only applies to the investigative process and meeting legal and court requirements. Completeness of information does not apply as other processes outside the investigation establish completeness. For example: data from tax forms or other IRS systems are accepted as recorded elsewhere, the same for information from subpoenas and search warrants.

25. 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

25a. 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.

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.

ATLAS is unscheduled. A request for records disposition authority for ATLAS and associated records will be drafted with the assistance of the IRS Records and Information Management (RIM) Program Office. When approved by the National Archives and Records Administration (NARA), disposition instructions for ATLAS inputs, system data, outputs and system documentation will be published in IRS Document 12990 under Records Control Schedule 30 for Criminal Investigation (item number to be determined), when next updated. A 10-year disposition (after case closure) has been tentatively proposed for ATLAS case file data

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.
Much of the security for the system is inherited from the CI-1 GSS where it is hosted. The GSS has undergone SA&A and has all appropriate controls, documentation, categorization, PIA and authorization in place.

26a. Next, explain how the data is protected in the system at rest, in flight, or in transition.

Data at rest on workstations is protected by the IRS approved hard drive encryption. Data at rest on servers is protected by IRS approved controls to include physical access restrictions and least privilege. Data in transmission is encrypted at two levels, on by the IRS WAN and the second by the CI router to router encryption using CISCO DMVPN

27. Has a risk assessment (e.g., SA&A) been conducted on the system to ensure that appropriate security controls have been identified and implemented to protect against known risks to the confidentiality, integrity and availability of the PII? No

28. Describe the monitoring/evaluating activities undertaken on a regular basis to ensure that controls continue to work properly in safeguarding the PII.

All operating and database controls are monitored regularly through the use of compliance checkers (WPC), vulnerability scanners (nCircle, Guardium) which are IRS mandated.

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? No

29a. Has approval been received from the Office of Privacy Compliance to use Live Data in testing (*if appropriate)*?

29b. If you have received permission from the Office of Privacy Compliance to use Live Data, when was the approval granted?

H. PRIVACY ACT & SYSTEM OF RECORDS

Under the statute, any employee who knowingly and willfully maintains a system of records without meeting the Privacy Act notice requirements is guilty of a misdemeanor and may be fined up to $5000.

Authority: OMB M 03-22 & Privacy Act, 5 U.S.C. 552a (e) (4) & PVR #13-Transparency

30. Are 10 or more records containing PII maintained/stored/transmitted through this system? Yes

31. Are records on the system retrieved by any identifier for an individual? (Examples of identifiers include but are not limited to Name, SSN, Photograph, IP Address) Yes

31a. If **YES**, the System of Records Notice(s) (SORN) published in the Federal Register adequately describes the records as required by the Privacy Act? Enter the SORN number and the complete name of the SORN.

SORN Number	SORN Name
Treas/IRS 46.002	Criminal Investigation Management Information Syst
Treas./IRS 34.037	IRS Audit Trail and Security Records System

I. ANALYSIS

Authority: OMB M 03-22 & PVR #21- Privacy Risk Management

32. What choices were made or actions taken regarding this IT system or collection of information as a result of preparing the PIA?

Resulted in the removal of PII from the system (e.g., SSN use reduced/eliminated)	No
Provided viable alternatives to the use of PII within the system	Yes
New privacy measures have been considered/implemented	Yes
Other:	No

32a. If **Yes** to any of the above, please describe:

NA