

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: October 22, 2014

PIA ID Number: **889**

---

1. What type of system is this? Modernized System

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

---

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

Automated Freedom of Information Act, AFOIA

---

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: 100,000 - 1,000,000

---

## 4. Responsible Parties:

---

NA

---

## 5. General Business Purpose of System

---

All federal agencies, including the Internal Revenue Service (IRS), are required under the Freedom of Information Act (FOIA) to disclose records requested in writing by any person (minus certain exemptions or exclusions). The Automated Freedom of Information Act (AFOIA) system was developed to assist the IRS in managing both the workload and the data involved in complying with this act. The AFOIA system development contract is with California Analysis Center, Inc. (CACI) Enterprise Solutions, Inc., located in Lanham, MD, and is comprised primarily of Commercial-Off-the-Shelf (COTS) products. The software is customized to meet all Governmental Liaison, Disclosure, & Safeguards (GLDS) business requirements (and data capture) for processing disclosure casework under Internal Revenue Code (IRC) 6103, FOIA, and to comply with the Privacy Act. Additionally, AFOIA provides administrative controls for other GLDS program work (e.g., governmental liaison programs), including daily time tracking by activity code for all GLDS employees, and generation of statistical management reports including work plan monitoring and balance measures performance results. The AFOIA system is comprised of the following three modules or components: Case Work, Program Work, and Agency Work. Case work consists of work flows and cases that must be worked by Disclosure employees. Program work generally covers quality reviews, disclosure awareness briefs, and disclosure questions or inquiries. This module determines the extent of tasking that can be provided, and identifies any information or services that can be provided. Agency work consists of activities relating to agencies outside of IRS. GLDS is within the Privacy, Governmental Liaison and Disclosure (PGLD), formerly the Office of Privacy, Information Protection and Data Security (PIPDS), organization under Operations Support. GLDS processes requests by persons, including local, state and federal agencies for tax information. These requests are processed through the Case Work functionality. Due process is provided pursuant to 5 USC.

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: 3/28/2012 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) Yes
- System is undergoing Security Assessment and Authorization No

---

6c. State any changes that have occurred to the system since the last PIA  
AFOIA system is no longer FISMA reportable. Also all POC information is being updated.

---

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'. 015-45-01-13-02-2581-00

---

**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	<u>Yes</u>	
Employees/Personnel/HR Systems	<u>Yes</u>	
Other	<u>Yes</u>	<u>Other Source: Requester, Copy Contractor</u>

- 
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	No
Address	Yes	Yes	Yes
Date of Birth	No	No	No

Additional Types of PII: Yes

**PII Name** On Public? On Employee?

sample      No              No

- 
- 10a. What is the business purpose for collecting and using the SSN ?  
The system stores tax and employment data necessary to comply with request for information under FOIA, Privacy Act, and IRC 6103.

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.)  
5 USC 552, 26 USC 6103, 5 USC 552a, 26 CFR 601.702; 26 CFR 301.6103
-

---

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

No alternative solution has been considered; the application requires the SSN to be able to respond to the request. The SSN number is needed to research and locate records in response to the request.

---

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 known mitigation strategy planned to eliminate the use of SSN for the system; SSN is required for the use of this system. The SSN number is needed to research and locate records in response to the request.

---

Describe the PII available in the system referred to in question 10 above.

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.

The AFOIA system audit trail track the following data elements: Action, category, computer name, date, item ID, item type, changes (New value and old value), and users.

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:

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA &amp; A?</u>	<u>Authorization Date</u>
IDRS	Yes	07/12/2011	Yes	03/10/2009
IMF	Yes	11/10/2009	Yes	03/08/2010
BMF	Yes	03/16/2010	Yes	06/14/2010
IMF	Yes	11/10/2009	Yes	03/08/2010
BMF	Yes	03/16/2010	Yes	06/14/2010
IDRS	Yes	07/12/2011	Yes	03/10/2009

b. Other federal agency or agencies: Yes

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

FRC

c. State and local agency or agencies: Yes

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

State Revenue Agencies

d. Third party sources: Yes

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

Copy Contractor

e. Taxpayers (such as the 1040): No

f. Employees (such as the I-9): No

g. Other: Yes If **Yes**, specify: Requester



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"?

The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

20. Did any of the PII provided to this system originate from any IRS issued forms? No

20b. If **No**, how was consent granted?

Written consent	<u>No</u>
Website Opt In or Out option	<u>No</u>
Published System of Records Notice in the Federal Register	<u>Yes</u>
Other:	<u>No</u>

---

## 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:

	<b>Yes/No</b>	<b>Access Level</b>
IRS Employees:	<u>Yes</u>	
Users		<u>Read Write</u>
Managers		<u>Read Write</u>
System Administrators		<u>No Access</u>
Developers		<u>No Access</u>
Contractors:	<u>No</u>	
Contractor Users		<u></u>
Contractor System Administrators		<u></u>
Contractor Developers		<u></u>
Other:	<u>No</u>	<u></u>

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?

When a new user needs access to IRS systems or applications, the user's manager or designated official, accesses the OL5081 application to request access for the new user. The completed OL5081 is submitted to the application administration approval group, and then an AFOIA user is added by their SEID. Access to the data within the application is restricted. Users are restricted to only those pieces of the application to which they need access by permissions and workgroup assignments. Users such as case workers only have access to input data for their work group assignment, run pre-programmed reports and ad hoc queries, and cannot delete data or records or manipulate or physically access the data. Access to the data tables is restricted to the application, system, and database administrators.

---

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

The source of the PII input into the system is the letter provided by the requester seeking access to records. Name, address, and other identifying information is provided to assist in locating the requested information and responding to the request. A number of fields have input and user validation measures to reduce errors. The case number is auto generated during indexing. In addition, the dates, SSN, Employer Identification Number (EIN), Years, and other similar fields for which users enter information have specifications for data formats and types. When entered incorrectly the user may be presented with an error message. In addition, employees working a particular case can verify with the IDRS, whether it does or does not have a record relating to that case. The case worker has to be an authorized user and have an account for IDRS. IDRS does not interconnect with AFOIA.

---

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? Yes

---

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.

AFOIA data retention requirements follow Records Control Schedule (RCS) 8, item 53 for FOIA Request Files and replace/supersede the Electronic Disclosure Information Management System (eDIMS) data retention requirements for Disclosure case work approved under National Archives Job No. N1-58-12-5 and published under RCS 8, item 42. PGLD and the Records Office will work together to update RCS 8 to appropriately reflect current aFOIA functionality and to update non-current system references and outdated work processes associated with aFOIA recordkeeping.

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.

---

26. Describe how the PII data in this system is secured, including appropriate administrative and technical controls utilized.

AFOIA follows all requirements in IRM 10.8.1.5.4.6(12), such as printing documents only necessary and required to support business processes, and implementing security principles such as least privileges. AFOIA follows the concept of least privilege, and access controls are implemented according to IRM 10.8.1 to protect the confidentiality and integrity of information at rest; users can only access information necessary to perform their job function. The application adheres to the SA&A and physical security requirements set forth in IRM 10.4.1- Physical Security Program- Managers Security Handbook.

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

AFOIA follows all requirements in IRM 10.8.1.5.4.6(12), such as printing documents only necessary and required to support business processes, and implementing security principles such as least privileges. AFOIA follows the concept of least privilege, and access controls are implemented according to IRM 10.8.1 to protect the confidentiality and integrity of information at rest; users can only access information necessary to perform their job function. The application adheres to the SA&A and physical security requirements set forth in IRM 10.4.1- Physical Security Program- Managers Security Handbook.

---

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? Yes

---

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

AFOIA stakeholders meet prior to any major change being made to the AFOIA application or system environment. Before changes are made, they are evaluated against the business requirements, which are generated and approved by application stakeholders. Specific planning and coordination occurs before conducting security-related activities affecting the information system. Appropriate planning and coordination between MITS Cybersecurity, the MITS Certification Program Office (CPO), MITS IT Security Architecture and Engineering (ITSAE), and the AFOIA Stakeholders occur before conducting these activities to minimize the impact on the AFOIA operations. On an annual basis, the business unit participates in the Tabletop and Enterprise Continuous Monitoring Exercises,

including updates to the Information Security Contingency Plan (ISCP) and SSP. Every three years, AFOIA will go through the SA&A process, which, in addition to the annual exercises, includes a comprehensive Security Control Assessment (SCA). When security audits, Security Control Assessment (SCA)'s, Security Impact Assessments (SIA), Security Risk Assessments (SRA) or certification activities are required, the Security PMO, MITS Security Assessment Services (SAS) and MITS Cybersecurity communicate with the Business Unit to ensure that they understand the scope of the security activity to be conducted.

---

29. Is testing performed, in accordance with Internal Revenue Manual (IRM) 10.8.8 - *IT Security, Live Data Protection Policy*? Not Applicable

---

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.

No SORN Records found.

## 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)	<u>No</u>
Provided viable alternatives to the use of PII within the system	<u>No</u>
New privacy measures have been considered/implemented	<u>Yes</u>
Other:	<u>No</u>

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

AFOIA system interfaces with the EAIB NTIN system to validate search requests for taxpayer data.