Date of Approval: 11/03/2017 PIA ID Number: **2954**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Automated Freedom of Information Act, AFOIA

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.

AFOIA, PIA #889

Next, enter the **date** of the most recent PIA. 11/13/2014

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? No

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. 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 comprised primarily of Commercial-Off-the-Shelf 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 (PA). 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). 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.

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 Yes On Spouse Yes 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)
Yes	Individual Taxpayer Identification Number (ITIN)
No	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	Practitioner Tax Identification Number (PTIN)

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSNs (or tax identification numbers). The Office of Management and Budget Circular 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 AFOIA system requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer for intergovernmental communications. SSNs are permissible from IRC 6109, which requires individual taxpayers to include their SSNs on their income tax returns. There is no known mitigation strategy planned to eliminate the use of SSNs for the system. The SSN is required for the use of this system. The SSN number is needed to research and locate records in response to the request. That said, the display of SSN/EIN information on the user screens is masked.

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.

Selected	PII Element	On Primary	On Spouse	On Dependent
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
Yes	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
Yes	Criminal History	No	No	No
Yes	Medical Information	No	No	No
Yes	Certificate or License Numbers	No	No	No
Yes	Vehicle Identifiers	No	No	No
Yes	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
Yes	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
Yes	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

Selected	SBU Name	SBU Description
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
Yes	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.
Yes	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
Yes	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.

6d. Are there other types of SBU/PII used in the system? No

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
Yes SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
Yes 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. The PII needed in this system allows GLDS employees to manage and respond to requests for access to IRS records. Requests can be made under the FOIA, PA, or IRC 6103. The application requires the SSN to be able to accurately respond to the request. The SSN number is needed to research and locate records in response to the request made under FOIA.

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 source of the PII inputted into the system is the letter provided by the requester seeking access to records. The requester is also required to provide proof of identity for verification. 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, 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 Integrated Data Retrieval System (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.

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
48.001	Disclosure Records
34.037	Audit trail and Security Records
24.030	IMF
26.046	BMF
36.003	General Personnel and Payroll Records
34.013	Identification Media Files System for Employees an
00.001	Correspondence Files and Correspondence Control Fi
00.008	Recorded Quality Review Records
22.062	Electronic Filing records
36.001	Appeals, Grievances and Complaints Records
37.006	Correspondence Miscellaneous Records and Information

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. ## Official Use Only

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.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
Business Master File (BMF)	Yes	04/24/2015	Yes	03/13/2013
Individual Master File (IMF)	Yes	03/06/2017	Yes	11/14/2016
Integrated Data Retrieval System (IDRS)	Yes	08/29/2017	Yes	12/21/2016

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

If **yes**, for each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
FED = Federal	Email or Secure Data Transfer (SDT)	Yes

11c. Does the system receive SBU/PII from State or local agency(s)? Yes

If **yes**, for each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
DOR = Department of Revenue	E-mail or Secure Data Transfer	Yes

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

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
706	United States Estate Tax Return
11-C	Occupational Tax and Registration Return for Wagering
709	United States Gift (and Generation-Skipping Transfer) Tax Return
720	Quarterly Federal Excise Tax Return
926	Return by a U.S. Transferor of Property to a Foreign Corporation
940	Employer's Annual Federal Unemployment (FUTA) Tax Return
941	Employer's Quarterly Federal Tax Return
943	Employer's Annual Federal Tax Return for Agricultural Employees
944	Employer's Annual Federal Tax Return
945	Annual Return of Withheld Federal Income Tax
990	Return of Organization Exempt from Income Tax
1040	US Individual Income Tax Return
1041	U.S. Income Tax Return for Estates and Trusts
1042	Annual Withholding Tax Return for U.S. Source Income of Foreign Persons
1065	U.S. Return of Partnership Income
1120	U.S. Corporation Income Tax Return

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? Yes

If **yes**, identify the forms

Form Number	Form Name
6166	Certification Program Letterhead

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? No

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

12c. Does this system disseminate SBU/PII to State and local agencies? Yes

If **yes**, identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
DOR = Department of Revenue	E-mail or Secure Data Transfer	Yes

Identify the authority and for what purpose? Agency data exchanges are for the purpose of tax administration or for 6103(i) to assist with investigations of Federal crimes. 26 CFR 301.6103 - IRC Section 6103 • 6103(d) Disclosure to state tax officials and state and local law enforcement agencies • 6103(h) Disclosure to certain Federal officers and employees for purposes of tax administration, etc. • 6103(i) Disclosure to federal officers or employees for administration of Federal laws not relating to tax administration The 6103(d) exchanges between state and local agencies are defined by a state or local agency specific Basic Agreement and Implementing Agreement. • Internal Revenue Manual (IRM) 11.3.32.5 Basic Agreements - The basic agreement provides for the mutual exchange of tax data between a specific state tax agency and the IRS. The provisions of the basic agreement encompass required procedures and safeguards. • IRM 11.3.32-3 Implementing Agreements - The purpose of this agreement is to provided implementing procedures for the Agreement on Coordination of Tax Administration between the IRS and xxxxxxxx (hereafter referred to as the "Agency.")

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? Yes

If **yes**, identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
CACI	Direct use of IRS Systems as Necessary	No

Identify the authority and for what purpose? Contractor support is required for planning, managing, and executing the design, build, test, and deployment phases of the proposed system. As such, the contractor will be expected to finalize business requirements, develop necessary design specifications, modify the application to meet requirements, develop and execute software testing and data validation to ensure quality deliverables, develop and execute a plan for data conversion, provide system documentation for operation and maintenance support, provide assistance as needed with any a Federal Information Security Management Act (FISMA)/Information Technology (IT) security activities and documentation. PA NOTIFICATION (APR 1984) The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the PA of 1974, Public Law 93-579, December 31, 1974 (5 United States Code (USC) 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties. In accordance with Homeland Security Presidential Directive 12, the Department of the Treasury Security Manual, Chapter II, Section 2, Investigative Requirements for Contractor Personnel describes "investigative requirements for contract employees, subcontractors, experts, and consultants who require staff-like access, wherever the location, to (1) Treasury/bureau-owned or controlled facilities; or (2) work on contracts that involve the design, operation, repair or maintenance of information systems; and/or (3) require access to sensitive but unclassified information." IRM 10.8.1, IT Security Policy and Guidance, establishes comprehensive, uniform security policies for the IRS. This manual applies to individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate IT systems containing IRS data. Pursuant to IRS Acquisition Procedure clause IR1052.239-9007, the contractor is required to furnish the Contracting Officer's Representative (COR) a list of names (as well as any other requested, supporting information) of new or substitute contractor employees and the IRS locations for which access is requested. A security screening, if determined appropriate by the IRS and in accordance with IRM 10.23.2, Personnel Security, Contractor Investigations, and Treasury Directive Publication 15-71, Chapter II, Section 2, will be conducted by IRS for each contractor employee requiring access to IRS' IT systems, or as otherwise deemed appropriate by the COR. Unless otherwise stated in Treasury regulation, the information shall be submitted within five days of contract award and within 24 hours of the date that the identity of a prospective personnel substitution has been confirmed. In addition to the requirements set forth above, the contractor shall also comply with the following IRS clauses: 1. IR1052.204-9003, IRS Security Awareness Training Requirements 2. IR1052.204-9005, Submission of Security Forms and Related Materials 3. IR1052.204-9006, Notification of Change in Contractor Employee Employment Status, Assignment, or Standing 4. IR1052.239-9007, Access, Use or Operation of IRS IT Systems by Contractors

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?
Yes

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, 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? In order to make a request under the FOIA, the source of the PII inputted into the system is a letter provided by the individual 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. Notice, consent and due process are provided pursuant to 5 USC.

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? The information collected under the FOIA is required to perform the search of requested records. Individuals do not have the opportunity to decline from providing the required information. In order to initiate a FOIA request the guidelines laid out in the "How to file a FOIA" section of the Internal Revenue website explicitly states the following: IRS has prepared a document at Appendix A- "How to Make a Freedom of Information Act Request" that describes the request process in greater detail. A requester who follows the IRS's specific procedures may receive a faster response. There are four basic elements to a FOIA request letter: First, the letter should state that the request is being made under the FOIA. Second, the request should identify the records that are being sought as specifically as possible. Third, the name and address of the requester must be included along with a copy of the requester's driver's license or a sworn or notarized statement swearing to or affirming their identity if the request involves the tax records of an individual or a business. In this case, the authority of the requester to receive such records must be established. NOTE: FOIA requests seeking a Centralized Authorization File Client Listing must attach a valid photo identification, including a signature. IRS will accept no other method of establishing identity for these requests. Fourth, the requester should make a firm commitment to pay any fees which may apply (the complete regulatory requirements for FOIA requests filed with the IRS are available at 67 Federal Register 69673, Treasury Regulation 601.702).

19. How does the system or business process ensure due process regarding information access, correction and redress? The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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 Contractor 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 and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Read And Write

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read and Write	High
Contractor Managers	Yes	Read and Write	High
Contractor Sys. Admin.	No		
Contractor Developers	No		

21a. How is access to SBU/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 Online 5081 (OL5081) application to request access for the new user. The completed OL5081 is submitted to the application administration approval group, and then the user is added by their Standard Employee Identifier. 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.

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? Yes

22a. 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. The system data retention requirements follows the following Records Control Schedule (RCS): 1. Access and disclosure request files, Case files created in response to FOIA requests a.) General Records Schedule (GRS) 4.2/020 ; Case files created in response to requests for information under the FOIA, Mandatory Declassification Review process, PA, Classification Challenge, and similar access programs (Job No. DAA-GRS-2013-0007-0002) b.) Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use. 2. Requests for Return and Return Information Files; Files consist of requests for copies or inspection of confidential tax returns or return information; either hard copy or tape extracts, and related records or actions taken (Job No. N1-58-05-2, Item 52) a.) RCS 8/52; Implementation Agreements and Memoranda of Understanding. b.) PGLD facilitates the exchange of data and fosters partnerships with federal, state, and local governmental agencies to improve tax administration, in accordance with Policy Statement 11-98, Fed-State Relations. See IRM 1.2.19.1.13, Policy Statement 11-98 (Formerly P-6-14). 3.) Disclosure of Information to Federal, State, and Local Agencies (DIFSLA). a.) Matching and Extract Program RCS 19/58 DIFSLA matching and extract program was developed pursuant to IRC 6103(1)(7) and IRC 6103(1)(7)(8) and includes Federal and State agencies authorized to participate in the program. Regarding Safeguards segment, the status of Safeguards reports/case files already scheduled under Job No. N1-58-00-1, and published in IRS Document 12990 under RCS 8, item 101.

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? 3/28/2012

23.1 Describe in detail the system s audit trail. The AFOIA system audit trail tracks the following data elements: action, category, computer name, date, item identification, item type, changes (New value and old value), and users. AFOIA is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **no**, please explain why. No, AFOIA system is no longer FISMA reportable. The AFOIA system is already in existence and does not require testing by IT. Any updates to the system is tested within the vendor test environment prior to moving into live production.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: 100,000 to 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? Yes

27a. If **yes**, explain the First Amendment information being collected and how it is used. While systems do not collect this information exclusively, the tax returns stored in the database will include information related to First Amendment rights, such as charitable contributions or income/deductions for such activities.

27b. If **yes**, please check all of the following exceptions (any one of which allows the maintenance of such information) that apply:

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance (as noted in Q17). No

The information maintained is pertinent to and within the scope of an authorized law enforcement activity. (As noted in Q7) No

There is a statute that expressly authorizes its collection. (Identified in Q6) Yes

27c. If **yes**, will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges? 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? Yes

If **yes**, does the system have a process in place to account for such disclosures in compliance with IRC 6103 (p) (3) (A) or Subsection (c) of the Privacy Act? Contact *Disclosure* to determine if an accounting is required. Yes

End of Report