Date of Approval: **November 24, 2020**

PIA ID Number: **5587**

SYSTEM DESCRIPTION

Enter the full name and acronym for the system, project, application and/or database.

Automated Freedom of Information Act, AFOIA

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Automated Freedom of Information Act, AFOIA, O&M, PCLIA#2954

What is the approval date of the most recent PCLIA?

11/3/2017

Changes that occurred to require this update:

Expiring PCLIA

Were there other system changes not listed above?

No

What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

The AFOIA Governance Board consists of the Associate Directors of Disclosure, Governmental Liaison, Safeguards and Data Services. The AFOIA Project Manager obtains approval from this Board for any functionality changes or additions to the AFOIA software.

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e. system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

GENERAL BUSINESS PURPOSE

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 workflows 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.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

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

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Interfaces with external entities that require the SSN

When there is no reasonable alternative means for meeting business requirements

Delivery of governmental benefits, privileges, and services

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued 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 SSNs 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.

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

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.

Employer Identification Number

Other Taxpayer Identification Number

Does this system use, collect, receive, display, store, maintain or disseminate other (non-SSN) PII (i.e. names, addresses, etc.)?

Yes

Specify the PII Elements:

Name

Mailing address

Phone Numbers

E-mail Address

Date of Birth

Standard Employee Identifier (SEID)

Protection Personal Identification Numbers (IP PIN)

Criminal History

Medical Information

Certificate or License Numbers

Vehicle Identifiers

Passport Number

Financial Account Numbers

Photographic Identifiers

Biometric Identifiers

Employment Information

Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List.

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

Procurement sensitive data Contract proposals, bids, etc.

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.

Proprietary data Business information that does not belong to the IRS

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

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

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 Freedom of Information Act (FOIA), Privacy Act (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.

How is the SBU/PII verified for accuracy, timeliness and completion?

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.

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.

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

Identify the Privacy Act SORN(s) that cover these records.

IRS 48.001 Disclosure Records

IRS 34.037 Audit Trail and Security Records

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 36.003 General Personnel and Payroll Records

IRS 34.013 Identification Media Files System for Employees and Others Issued IRS Identification

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 00.008 Recorded Quality Review Records

IRS 22.062 Electronic Filing Records

IRS 36.001 Appeals, Grievances and Complaints Records

IRS 37.006 Correspondence, Miscellaneous Records, and Information Management Records

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

Does the system receive SBU/PII from other systems or agencies?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Business Master File (BMF)
Current PCLIA: Yes
Approval Date: 4/24/2015
SA&A: Yes
ATO/IATO Date: 3/13/2013

System Name: Individual Master File (IMF)
Current PCLIA: Yes
Approval Date: 3/6/2017
SA&A: Yes
ATO/IATO Date: 11/14/2016

System Name: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 8/29/2017
SA&A: Yes
ATO/IATO Date: 12/21/2016

Does the system receive SBU/PII from other federal agency or agencies?

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).

Name: FED=Federal Agencies
Transmission Method: Email or Secure Data Transfer (SDT)
ISA/MOU: Yes

Does the system receive SBU/PII from State or local agency (-ies)?

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: DOR=Department of Revenue
Transmission Method: Email or Secure Data Transfer
ISA/MOU: Yes

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 706 Form Name: Unites State Estate Tax Return

Form Number: 11-C Form Name: Occupational Tax and Registration Return for Wagering

Form Number: 709 Form Name: Unites States Gift (and Generation-Skipping Transfer) Tax Return

Form Number: 720 Form Name: Quarterly Federal Excise Tax Return

Form Number: 926 Form Name: Return by a U.S. Transferor of Property to a Foreign Corporation

Form Number: 940 Form Name: Employer's Annual Federal Unemployment (FUTA) Tax Return

Form Number: 941 Form Name: Employer's Quarterly Federal Tax Return

Form Number: 943 Form Name: Employer's Annual Federal Tax Return for Agricultural Employees

Form Number: 944 Form Name: Employer's Annual Federal Tax Return

Form Number: 945 Form Name: Annual Return of Withheld Federal Income Tax

Form Number: 990 Form Name: Return of Organization Exempt from Income Tax

Form Number: 1040 Form Name: US Individual Income Tax Return

Form Number: 1041 Form Name: U.S. Income Tax Return for Estates and Trusts

Form Number: 1042 Form Name: Annual Withholding Tax Return for U.S. Source Income of Foreign Persons

Form Number: 1065 Form Name: U.S. Return of Partnership Income

Form Number: 1120 Form Name: U.S. Corporation Income Tax Return

Form Number: 6166 Form Name: Certification Program Letterhead

Does the system receive SBU/PII from Employee forms (e.g. the I-9)?

Yes

Please identify the form number and name:

Form Number: 6166 Form Name: Certification Program Letterhead

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

No

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

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

Identify the authority

Internal Revenue Manual (IRM) 1.2.2.11.2 Delegation Order 11-2 (Rev.3), Authority to Permit Disclosure of Tax Information and to Permit the Production of Documents - The purpose of this is to share return information with the Department of Justice in relation to tax administration and nontax criminal investigations or to locate fugitives. IRM 11.3.32-3 Implementing Agreements - The purpose of this agreement is to provide implementing procedures for the Agreement on Coordination of Tax Administration between the IRS and XXXXXXXX (hereafter referred to as the "Agency”).

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

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(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.

For what purpose?

Agency data exchanges are for the purpose of tax administration or to assist with investigations of Federal crimes including disclosure to federal officers or employees for administration of Federal laws not relating to tax administration.

Does this system disseminate SBU/PII to State and local agencies?

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: DOR=Department of Revenue
Transmission Method: Email or Secure Data Transfer (SDT)
ISA/MOU: Yes

Identify the authority.

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 provide implementing procedures for the Agreement on Coordination of Tax Administration between the IRS and XXXXXXXX (hereafter referred to as the "Agency").

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

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.

For what purpose?

Agency data exchanges are for the purpose of tax administration or to assist with investigations of Federal crimes including disclosure to federal officers or employees for administration of Federal laws not relating to tax administration and exchanges between state and local agencies are defined by a state or local agency specific Basic Agreement.

Does this system disseminate SBU/PII to IRS or Treasury contractors?

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: CACI
Transmission Method: Direct use of IRS Systems as Necessary
ISA/MOU: No

Identify the authority.

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.

For what purpose?

Yes

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

Yes

Does this system disseminate SBU/PII to other Sources?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

No

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or 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.

Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information?

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).

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.

INFORMATION PROTECTION

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

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Write

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.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series 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, FedState 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.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

Yes

What date was it completed?

3/28/2012

Describe 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.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

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 are tested within the vendor test environment prior to moving into live production.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Under 5,000

Members of the Public: 100,000 to 1,000,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

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.

Please list all exceptions (any one of which allows the maintenance of such information) that apply:

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

Will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges under Federal programs?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

No

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

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

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