Date of Approval: **February 05, 2024**

PIA ID Number: **8178**

SYSTEM DESCRIPTION

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

eGain Solve - Secure Message, eGain - SM

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?

Taxpayer Digital Communications, TDC #5188

What is the approval date of the most recent PCLIA?

7/7/2020

Changes that occurred to require this update:

Significant Merging with Another System

New Access by IRS employees or Members of the Public

Were there other system changes not listed above?

Yes

What were those changes?

Note: When the prior PCLIAs were created (#5188, #3470, #801), the Taxpayer Digital Communications (TDC) Program Office in the business unit Office of Online Services (OLS) implemented this solution and labeled the program "TDC". In early 2021, the managed service contract transitioned to IT UNS CCSD who references the program as eGain. Hence, the terms TDC and eGain are used interchangeably. In addition, for purposes of clearly communicating to the public the various components of eGain offered in the Service, the PCLIA is being split into three (3): one for Secure Messaging, one for Chat and one for Virtual Assistant. In April 2023, Secure Messaging integrated with WebApps Enterprise Services, WAES (aka Online Account OLA) to enable individuals to view and respond to Secure Messages within their Online Account.

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

User and Network Services (UNS) Governance Board & Strategic Development Executive Steering Committee (ESC)

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?

Yes

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.

eGain Platform: The Internal Revenue Service began offering digital communication with taxpayers and representatives in 2016. The Service utilizes eGain Solve™, an omnichannel customer engagement software suite which is implemented as a Managed Services solution, hosted in an Amazon Web Services (AWS) GovCloud private cloud environment. The eGain Solve™ software suite provides the opportunity to exchange communique and information between IRS Assistors and taxpayers/authorized representatives using Secure Messaging, Chat, and/or Virtual Assistant (aka Chatbot). Secure Messaging: Secure messaging creates secure message centers for taxpayers, their representatives, and other third parties. Once authenticated, a taxpayer can log into their inboxes in the Secure Message Center to view or respond to messages with IRS employees, who can then reply on the same secure channel. This helps ensure that sensitive information shared during this exchange between IRS employee and taxpayer are not exposed to external networks and are thus put at less risk. Secure messages do not interact with mail servers and are used to communicate sensitive and/or important information in a secure environment. For IRS employees, secure messages are handled by workflows, which direct incoming messages to the appropriate IRS employee who logs in to the secure message center to manage messages. For taxpayers and their authorized representatives, secure messages can only be accessed after they have signed into their Secure Messaging portal, which is only accessible by authenticated customers. When a taxpayer is sent a new secure message, they receive a notification informing them that there is a message for them in the Secure Messaging Center. In order to read the message, they must log in to their secure message center. Secure messages cannot leave the application and cannot be viewed by customers unless they have authenticated.

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:

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Another compelling reason for collecting the SSN

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

The eGain System requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer at this time. The use of SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. The SSN is passed by IRS Secure Access Digital Identity (SADI) during the authentication process for an individual taxpayer or Powers of Attorney. In addition, the data will be used to better understand the type of taxpayer who use the system and thus will allow the Service to make strategic decisions about how best to expand the secure messaging to other areas.

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

No mitigation strategy currently exists as the SSN is uniquely needed to identify a user's record. 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.

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
Place of Birth
Standard Employee Identifier (SEID)
Internet Protocol Address (IP Address)
Certificate or License Numbers
Vehicle Identifiers
Financial Account Numbers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

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.

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.

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

Yes

Describe the other types of SBU/PII that are applicable to this system.

Any information that is currently sent via domestic or international mail, phone call, fax, or provided in a face-to-face setting for any IRS interaction could be securely transmitted digitally via Secure Messaging if that information is in a digital format. This includes various

forms containing PII. System level information includes user ID's, case ID's, activity ID's, log files, activity dates, activity types, transaction logs, and audit events which could be considered SBU.

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

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.

Specific use of SBU/PII is based on the taxpayers and the IRS Business Operating Division (BOD) use case needs for Secure Messaging. eGain is a secure digital communication platform that allows multiple document types to be exchanged. These document types will contain the same or similar SBU/PII as what is currently contained in traditionally paper-based file sharing methods like correspondence via US or International mail, faxes, or documents provided via face-to-face meetings. Instead of these traditional methods, such documents will be sent and received either via Secure Message but only after the taxpayer or authorized representative has fully authenticated via IRS SADI or other approved methods such as a signed Consent Agreement.

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

IRS employees' access eGain to review and analyze any information that the taxpayer and/or representative sends in the secure message including electronically transferred attachments. The source of the SBU/PII is provided directly by the TP/POA. Accuracy and completeness is determined by the assigned IRS employee. When available, the IRS employee matches the information against internal databases (i.e., Integrated Data Retrieval System (IDRS)). Note: The IRS employee has to be an authorized user and have an account for IDRS; IDRS does not interconnect with eGain Secure Messaging. The timeliness of information received will be verified and assessed by the assigned IRS employee.

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 00.001 Correspondence Files and Correspondence Control Files

IRS 00.002 Correspondence Files: Inquiries about Enforcement Activities

IRS 00.003 Taxpayer Advocate Service and Customer Feedback and Survey Records

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 24.047 Audit Underreporter Case Files

IRS 26.009 Lien Files

IRS 26.012 Offer in Compromise Files

IRS 26.013 Trust Fund Recovery Cases/One Hundred Percent Penalty Cases

IRS 26.019 Taxpayer Delinquent Account Files

IRS 26.020 Taxpayer Delinquency Investigation Files

IRS 34.037 Audit Trail and Security Records

IRS 36.003 General Personnel and Payroll Records

IRS 42.001 Examination Administrative Files

IRS 42.021 Compliance Programs and Projects Files

IRS 44.001 Appeals Case Files

IRS 44.003 Appeals Centralized Data

IRS 50.001 Tax Exempt & Government Entities (TE/GE) Correspondence Control Records

IRS 50.003 Tax Exempt & Government Entities (TE/GE) Reports of Significant Matters

IRS 50.222 Tax Exempt/Government Entities (TE/GE) Case 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: Secure Access Digital Identity, SADI
Current PCLIA: Yes
Approval Date: 2/15/2023
SA&A: Yes
ATO/IATO Date: 6/6/2023

System Name: WebApps Enterprise Services, WAES (aka Online Account)
Current PCLIA: Yes
Approval Date: 11/7/2022
SA&A: Yes
ATO/IATO Date: 1/11/2023

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

No

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

No

Does the system receive SBU/PII from other sources?

Yes

Identify the source 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: Taxpayer / Representative
Transmission Method: Agent receives information from secure message
ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: F1040, related forms & schedules
Form Name: Individual Income Tax Return

Form Number: F1065, related forms & schedules
Form Name: Return of Partnership Income

Form Number: F1120, related forms & schedules
Form Name: Corporation Income Tax Return

Form Number: F1120S, related forms & schedules
Form Name: Income Tax Return for an S Corporation

Form Number: Other Forms & schedules
Form Name: Any tax computation form used in IMF & BMF

Form Number: Form 433F
Form Name: Collection Information Statement

Form Number: CP2000
Form Name: Initial Notice - Request Verification for Unreported Income, Deductions, Payments and/or Credits on

Form Number: CP2501
Form Name: Initial Contact - Potential Discrepancy of Income, Deductions and/or Credits Claimed on BMF Income T

Form Number: various forms by Collection
Form Name: various forms by Collection

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

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

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Security Audit and Analysis System (SAAS)
Current PCLIA: Yes
Approval Date: 7/31/2023
SA&A: Yes
ATO/IATO Date: 6/12/2023

System Name: Correspondence Examination Automation Support (CEAS)
Current PCLIA: Yes
Approval Date: 2/18/2021
SA&A: Yes
ATO/IATO Date: 1/27/2023

System Name: RAAS Compliance Data Warehouse (CDW)
Current PCLIA: Yes
Approval Date: 2/13/2023
SA&A: Yes
ATO/IATO Date: 5/12/2022

System Name: Appeals Centralized Database System (ACDS)
Current PCLIA: Yes
Approval Date: 3/2/2021
SA&A: Yes
ATO/IATO Date: 12/2/2022

System Name: Automated Underreporter (AUR)
Current PCLIA: Yes
Approval Date: 6/7/2022
SA&A: Yes
ATO/IATO Date: 1/27/2023

System Name: Issue Management System (IMS)
Current PCLIA: Yes
Approval Date: 10/17/2022
SA&A: Yes
ATO/IATO Date: 5/13/2022

System Name: Reporting Compliance Case Management System (RCCMS)
Current PCLIA: Yes
Approval Date: 10/14/2020
SA&A: Yes
ATO/IATO Date: 11/8/2022

System Name: Centralized Authorization File (CAF)
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 11/8/2022

System Name: WebApps Enterprise Services, WAES (aka Online Account OLA)
Current PCLIA: Yes
Approval Date: 7/7/2023
SA&A: Yes
ATO/IATO Date: 1/11/2023

Identify the authority.

The authority to disclose information is pursuant to section 6103(d) of the Internal Revenue Code (IRC). IRC 6103(d) provides for disclosure of returns and return information to any state agency, body or commission, or its legal representative charged under the laws of the state with the responsibility for administration of any state tax law.

For what purpose?

Tax Administration, as enacted by Internal Revenue Code Section 6201 Assessment of Taxes

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

No

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

No

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

No

Does this system disseminate SBU/PII to other Sources?

Yes

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

Organization Name: SPLUNK
Transmission Method: Secure Data transfer
ISA/MOU: No

Identify the authority.

The authority to disclose information is pursuant to section 6103(p)(3)(A) of the Internal Revenue Code (IRC).

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

Treasury/SORN 34.037 - IRC 6103(p)(3)(A) provides for disclosure of returns and return information and such inspection or disclosure shall be made in such manner and at such time and place as shall be prescribed.

For what purpose?

(p)Procedure and recordkeeping (3) Records of inspection and disclosure (A)System of recordkeeping. Audit and tracking log data will be posted to SPLUNK.

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?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

12/15/2021

Please identify the ownership of the CSP data.

Third Party

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

Does this system/application interact with the public?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Yes

When was the e-RA completed?

2/2/2023

What was the approved level of authentication?

Level 3: High confidence in the asserted identity's validity

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?

Upon first entry to the eGain platform, individuals must agree to a 'Terms of Service' (TOS) before continuing to use secure messaging. The TOS has been fully approved that IRS Counsel Office, IRS Privacy, Governmental Liaison and Disclosure group, and IRS Online Services. Any change to the TOS will require any current or new taxpayer that accesses the system to agree to updated language before continuing to use secure messaging. Terms Of Service & Rules of Conduct: https://www.irs.gov/help/irs-secure-messaging-terms-of-service-and-rules-of-conduct

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

An individual has the ability to decline using the system after reading the Terms of Service (TOS) and can opt not to proceed with the online session. Also, at any time, the taxpayer can refuse to provide any information via secure messaging and continue to use fax, mail, or in person communications.

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. Notice, consent, and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to Title 5 of the United States Code (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 Contractor Operated

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

IRS Employees

Users: Read Write
Managers: Read Write
System Administrators: Administrator

IRS Contractor Employees

Contractor Users: Read Write
Contractor System Administrators: Administrator

How is access to SBU/PII determined and by whom?

When a new user needs access to an IRS system or application, the employee submits a request for access through Business Entitlement Access Request System (BEARS) application; the user's manager, or designated official, approves or denies after review. The completed BEARS is then routed to an application administration approval group, and then the user account is added. 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. Agents (end users) only have access to input data for their own account, run pre-programmed reports and ad hoc searches. They can delete their own data but cannot manipulate or physically access the data belonging to another user. Access to data tables is restricted to the application, system, and database administrators. Developer(s) have no access to production systems. UNAX training is also provided to inform users of the statutory rules governing and the IRS' policy on unauthorized access and inspection of records by IRS employees. A management designee monitors system access and removes permissions when individuals no longer require access. User accounts are disabled and not deleted. Users are assigned to specific modules of the application and specific roles within the modules. Establishing an account follows the principle of least privilege, providing the least amount of access to PII/SBU data to accomplish his/her work.

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.

Some eGain data files are approved for deletion/destruction under the National Archives and Records Administration's (NARA) General Records Schedules (GRS). Records related to general customer service operations (administrative support) including communications with the public regarding status of customer support, tickets and tracking logs, reports on customer management data, customer feedback should be managed according to GRS 5.2, Item 020: Temporary. Disposition Instructions: Destroy when no longer needed for business use, or according to an agency predetermined time period or business rule. All other eGain case/business-specific records are currently unscheduled and cannot be deleted/destroyed from the eGain system until data retention rules are finalized and NARA-approved. To the greatest extent possible, case/business-specific records should be transferred from eGain and placed in business unit repositories for processing and management (disposition). The Records Office will continue working with the System Owner, IT, and business unit stakeholders to address system recordkeeping requirements, including the final disposition of eGain case-related data files that cannot be transferred off the system into business unit repository.

SA&A OR ASCA

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

In-process

When is the anticipated date of the SA&A or ACS completion?

5/1/2023

Describe the system's audit trail.

eGain has a Cybersecurity-approved audit plan last revised in Sept 2020. A complete audit trail of the use of the system is captured and ingested by SPLUNK. The system monitors for security risks and compliance violations to ensure that the use of the system takes place only for an approved purpose that is within the professional responsibility of each user It records all actions of the taxpayer/user in near-real-time and transmits to Enterprise Security Audit Trail (ESAT)/Security Audit and Analysis System (SAAS) logs for Cybersecurity review. The audit trail contains the audit trail elements as required in current 10.8.1.3.3, Audit and Accountability Policy and Procedures The content of the audit record includes the following data elements: USERID, USER TYPE, SYSTEM, EVENTID, TAXFILERTIN, TIMESTAMP (e.g., date and time of the event), ADDITIONAL APPLICATION DATA (action taken of user when creating the event). The following transactions fall under the criteria of an Auditable Event: Log onto the system [Log in, Session Created] (Success, Fail), Log off the system [Log out, Session Completed] (Success, Fail), all agents (privileged) events, all system and data interactions concerning Personally Identifiable Information (PII) and Sensitive but Unclassified (SBU), to include external user data [Session Created, Session

Completed, Session Timed Out] (Success, Fail) The collection and management of auditable data complies with IRS, Treasury, and other federal requirements which require the following data elements to be audited.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

eGain uses a Jira solution to track the configuration management decisions, supporting documentation, and approvals. Jira is a centralized solution that facilitates workflow, includes references to the code location, and contains test results from proposed changes. eGain uses a Subversion server to maintain version control. All configuration baselines are documented, stored in a SharePoint repository, and are version controlled with ability to refer previous versions.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

Describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?

The platform is in an approved and system tested state and is the responsibility of the managed service provider (MSP). Additional system testing is performed by both the MSP and the Service for each maintenance, change request and new-functionality releases in accordance with Internal Revenue Manual (IRM) 2.127.2, Testing Standards and Procedures, IT Testing Process and Procedures. The MSP performs testing to verify the implemented functionality meets the specified requirement which includes Unit Testing (UT), System Integration Testing (SIT), and / or Regression Testing. The Service is also provided a testing opportunity to validate that the implemented functionality satisfies the intended requirement and confirm applicable Privacy Requirements are met [User Acceptability Testing (UAT) and Regression Testing]. In addition, privacy validation activities occur such as: Internal agent user access reports are captured & reviewed. The Service collects only minimum

taxpayer information that is necessary for secure messaging. Unnecessary taxpayer profile information is not stored in the system. Minimum employee information is input and stored in the system for access and messaging with taxpayers. PII information input fields for are limited and controlled by system administrators to minimize the amount of PII that can be input into the system. Roles in the eGain Secure Messaging limit PII accessibility to only personnel with justification to view. Access to PII is controlled through role-based permissions to only required personnel. System access by IRS employee is controlled through PIV/SSO access with IRS network connection required. All changes to PII data are tracked in audit logs. The vendor performs testing to verify the implemented functionality meets the specified requirement which includes Unit Testing (UT), System Integration Testing (SIT), and/or Regression Testing. OLS also is provided a testing opportunity to validate that the implemented functionality satisfies the intended requirement and confirm applicable Privacy Requirements are met [User Acceptability Testing (UAT) and Regression Testing]. Changes to each environment require OLS/CCSD approval prior to implementation.

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?

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