Date of Approval: **02/05/2024** PIA ID Number: **8178**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. eGain Solve - Secure Message, eGain - SM

2. Is this a new system? No

2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

Taxpayer Digital Communications, TDC #5188

Enter the approval **date** of the most recent PCLIA. 07/07/2020

If **yes** Indicate which of the following changes occurred to require this update (check all that apply).

_____ Addition of Personally Identifiable Information (PII)(PII is any information that is linked or linkable).
_____ Conversions
_____ Anonymous to Non-Anonymous
_____ Significant System Management Changes
Yes Significant Merging with Another System
Yes New Access by IRS employees or Members of the Public
_____ Addition of Commercial Data / Sources
_____ New Interagency Use
_____ Internal Flow or Collection
_____ Expiring PCLIA

Were there other system changes not listed above? Yes

If **yes**, explain what changes were made. 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.

3. 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)

3.a. Check the current Enterprise Life Cycle (ELC) 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? Yes

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.
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.

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

6.a. 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 all types of tax identification numbers (TIN) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

	Security background investigations
	Interfaces with external entities that require the SSN
	Legal/statutory basis (e.g. where collection is expressly required by statute)
Yes	When there is no reasonable alternative means for meeting business requirements
Yes	Statistical and other research purposes
	Delivery of governmental benefits, privileges, and services
	Law enforcement and intelligence purposes
Yes	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

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.

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

If **yes**, specify the information.

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

No	Photographic Identifiers
No	Biometric Identifiers
Yes	Employment Information
Yes	Tax Account Information
Yes	Centralized Authorization File (CAF)

6.c. 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
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
No	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. Are there other types of SBU/PII used in the system? Yes

If **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.

6.e. 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

No	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
No	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

6.f. Has the authority been verified with the system owner? Yes

If the answer to 6f is **No**, verify the authority is correct with the system owner and then update the answer to 6f.

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.

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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

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.

C. 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.

9. 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

If **yes**, enter the SORN number(s) and the complete the name of the SORN(s).

SORNS Number	SORNS Name
Treasury/IRS 00.001	Correspondence Files and Correspondence Control Fi
Treasury/IRS 00.002	Correspondence Files: Inquiries about Enforcement
Treasury/IRS 00.003	Taxpayer Advocate Service and Customer Feedback an
Treasury/IRS 24.030	Customer Account Data Engine Individual Master Fil
Treasury/IRS 24.046	Customer Account Data Engine Business Master File
Treasury/IRS 24.047	Audit Underreporter Case Files
Treasury/IRS 26.009	Lien Files
Treasury/IRS 26.012	Offer in Compromise Files
Treasury/IRS 26.013	Trust Fund Recovery Cases/One Hundred Percent Pena
Treasury/IRS 26.019	Taxpayer Delinquent Account Files
Treasury/IRS 26.020	Taxpayer Delinquency Investigation Files
Treasury/IRS 34.037	Audit Trail and Security Records
Treasury/IRS 36.003	General Personnel and Payroll Records
Treasury/IRS 42.001	Examination Administrative Files
Treasury/IRS 42.021	Compliance Programs and Projects Files
Treasury/IRS 44.001	Appeals Case Files
Treasury/IRS 44.003	Appeals Centralized Data
Treasury/IRS 50.001	Tax Exempt & Government Entities (TE/GE) Correspon
Treasury/IRS 50.003	Tax Exempt & Government Entities (TE/GE) Reports o
Treasury/IRS 50.222	Tax Exempt & Government Entities (TE/GE) Case Mana
Treasury 00.015	General Information Technology Access Account Reco

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy .*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles.

System Owner (SES level or above)		Subject Matter Expert (SME)	
Name	Teresa Sabol	Name	Theresa Henry Ricks
Title	IT Program Manager	Title	Infor Technology Spec (INFOSEC)
Phone Number	202-283-0529	Phone Number	240-613-4335
Email Address	teresa.sabol@irs.gov	Email Address	theresa.h.ricks@irs.gov

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII data from other sources, forms, systems or agencies? Yes

11.a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Secure Access Digital Identity, SADI	Yes	02/15/2023	Yes	06/06/2023
WebApps Enterprise Services, WAES (aka Online Account)	Yes	11/07/2022	Yes	01/11/2023

11.b. Does the system receive SBU/PII from other federal agency or agencies? No

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). No Organization Records found.

11.c. Does the system receive SBU/PII from State or local agency (-ies)? No

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).
No Organization Records found.

11.d. Does the system receive SBU/PII from other sources? Yes

If **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	Transmission method	ISA/MOU
Taxpayer / Representative	Agent receives information from secure message	No

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

If **yes**, identify the forms.

Form Number	Form Name
F1040, related forms & schedules	Individual Income Tax Return
F1065, related forms & schedules	Return of Partnership Income
F1120, related forms & schedules	Corporation Income Tax Return
F1120S, related forms & schedules	Income Tax Return for an S Corporation
Other Forms & schedules	Any tax computation form used in IMF & BMF
Form 433F	Collection Information Statement
CP2000	Initial Notice - Request Verification for Unreported Income, Deductions, Payments and/or Credits on

CP2501	Initial Contact - Potential Discrepancy of Income, Deductions and/or Credits Claimed on BMF Income T
various forms by Collection	various forms by Collection

11.f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

If **yes**, identify the forms.
No Employee Form Records found.

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PCLIA	Approval Date	SA&A?	Authorization Date
Security Audit and Analysis System (SAAS)	Yes	07/31/2023	Yes	06/12/2023
Correspondence Examination Automation Support (CEAS)	Yes	02/18/2021	Yes	01/27/2023
RAAS Compliance Data Warehouse (CDW)	Yes	02/13/2023	Yes	05/12/2022
Appeals Centralized Database System (ACDS)	Yes	03/02/2021	Yes	12/02/2022
Automated Underreporter (AUR)	Yes	06/07/2022	Yes	01/27/2023
Issue Management System (IMS)	Yes	10/17/2022	Yes	05/13/2022
Reporting Compliance Case Management System (RCCMS)	Yes	10/14/2020	Yes	11/08/2022
Centralized Authorization File (CAF)	Yes	10/26/2021	Yes	11/08/2022
WebApps Enterprise Services, WAES (aka Online Account OLA)	Yes	07/07/2023	Yes	01/11/2023

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

12.b . Does this system disseminate SBU/PII to other Federal agencies? No
If **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)No Organization Records found.

Identify the authority.

Identify the routine use in the applicable SORN (or Privacy Act exception).

For what purpose?

12.c. Does this system disseminate SBU/PII to State and local agencies? No

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).
No Organization Records found.

Identify the authority.

Identify the routine use in the applicable SORN (or Privacy Act exception.)

For what purpose?

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

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).
No Organization Records found.
Identify the authority

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

If **no**, explain.

12.e. Does this system disseminate SBU/PII to other Sources? Yes

If **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	Transmission method	ISA/MOU
SPLUNK	Secure Data transfer	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.

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

13.a. If **yes**, have you conducted a Social Media PIA?

If **no**, Contact *Privacy for assistance with completing the Social Media PIA.

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No

14.a. If **yes**, briefly explain how the system uses the referenced technology.

15. Does the system use cloud computing? Yes

15.a. If **yes**, Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified? Yes

If **yes**, Date Certified. 12/15/2021

If **no**, please explain.

15.b. Please identify the ownership of CSP data. 3rd Party

Please identify the 3rd party. Amazon Web Services GovCloud

15.c. Does the CSP allow auditing? Yes

Who audits the CSP data? IRS

15.d. Please select background check level required for CSP. Moderate

15.e. Is there a breach/incident plan on file? Yes

If **no** When will Breach/incident plan be available

15.f. Privacy laws (including access and ownership) can differ in other countries. If any data is considered SBU, will this cloud be Continental US (CONUS) only for:

Storage	Yes
Transmission	Yes
Maintenance (including backups)	Yes
Troubleshooting	

16. Does this system/application interact with the public? Yes

16.a. If **yes**, was (or will) an electronic risk assessment (e-RA) conducted on the system/application? Yes

16.a.1. If **yes**, when was the **e-RA** conducted? 02/02/2023

If **yes**, what was the approved level of authentication?

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

If **Level 2**, Confidence based on:

If **no**, when will the e-RA be conducted?

If **Not Applicable**, explain why not required.

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? Yes

17.a. 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?
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

17.b. If **no**, why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

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

18.a. If **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.

18.b. If individuals do not have the opportunity to give consent, why not?

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. 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).

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	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Read and Write	Moderate
Contractor Managers	No		

Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	No		

21.a. 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.

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

22.a. 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 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.

22.b. If **no**, you must work with the IRS Records and Information Management (RIM) Program Office to address records retention requirements before you dispose of any records in this system.

I.2SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? In-process

23.a. If **yes**, what date was it completed?

23.b. If **in process**, when is the anticipated date of the SA&A or ASCA completion? 05/01/2023

23.c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

If **no**, please explain the process that was followed to ensure the system safeguards SBU/PII from unauthorized or inappropriate access. Include a description of the formalized documentation, process, and review that was used to analyze the system's security controls.

If **do not know**, please explain the process that was followed to ensure the system safeguards SBU/PII from unauthorized or inappropriate access. Include a description of the formalized documentation, process, and review that was used to analyze the system's security controls..

23.1 Describe in detail 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a If **yes**, If yes, was the test plan completed? Yes

If **no**, When is the test plan scheduled for completion?

24.a.1. If **yes**, where are 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.

24.a.2. If **yes**, were all the Privacy Requirements successfully tested? Yes

24.a.2.b. If **no**, please explain which Privacy requirements were not tested and why?

24.a.3. If **yes**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.a.3.a. If **yes**, please describe the outstanding issues.

24.b. If **no**, please explain why.

24.1. Describe what testing and validation activities which have been conducted or are in process 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.

K. SBU Data Use

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

25a. If **yes,** was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

If **yes,** provide the date the permission was granted.
If **no**, explain why not.

25.b. If **yes**, was testing performed in conformance with IRM 10.5.8, Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments?
If **no**, explain why not.

L. NUMBER AND CATEGORY OF PII RECORDS

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

26.a. IRS Employees:	Under 50,000
26.b. Contractors:	Under 5,000
26.c. Members of the Public:	100,000 to 1,000,000
26.d. Other:	No

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

27.a. If **yes**, explain the First Amendment information being collected and how it is used.

27.b. 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 Q 7) No
There is a statute that expressly authorizes its collection. (Identified in Q6) No

27.c. 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 under Federal programs?

If **yes**, explain the determination process. Consult with IRS General Legal Services to complete this section.

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?* No

If **yes**, provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable).

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

30. Does Computer matching occur? No

30.a. Does your matching meet the Privacy Act definition of a matching program?

30.b. Can the business owner certify that it meets requirements of IRM 11.3.39, Disclosure of Official Information, Computer Matching & Privacy Protection Act?

If **no**, Please explain

N. ACCOUNTING OF DISCLOSURES

31. 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

31.a. 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

31.b. If **no**, accounting of Disclosures risk noted. Contact Disclosure to develop accounting of disclosures. Explain steps taken to develop accounting of disclosures process.

31.c. If **N/A**, explain the Exemption and/or Disclosure s response.

End of Report