Date of Approval: 04/19/2025
Questionnaire Number: 2069

Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

eGain Solve - Secure Message, eGain - SM

Acronym:

eSSM

Business Unit

Information Technology

Preparer

For Official Use Only

Subject Matter Expert

For Official Use Only

Program Manager

For Official Use Only

Designated Executive Representative

For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

The Internal Revenue Service (IRS) utilizes eGain Solve™, an omnichannel customer engagement software suite which is implemented as a Managed Services solution, hosted in Federal Risk and Authorization Management Program (FedRAMP) 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 creates secure message centers for taxpayers, their representatives, and other third parties. Users are authenticated via The Secure Access Digital Identity (SADI) platform. SADI utilizes National Institute of Standards and Technology (NIST) Special Publication 800-63-3 compliant credential service provider (CSP) technology to enable people to securely access and use IRS online tools and applications. SADI utilizes CSP credentials to match users to their IRS account, pass the minimum amount of

identifying data to internal applications, and connect users to information they are authorized to review. 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. 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. This technology enables taxpayers to be directed to an appropriate IRS.gov landing page for assistance in lieu of calling the toll-free number. The taxpayer participation is voluntary. The benefits of this functionality align with the IRS strategic goal of improving service to make voluntary compliance easier for taxpayers. The eGain platform is linked to Tax Professional Account (Tax Pro), Clean Energy (ECO) Portal and the Direct File (DF) application. In all instances, the taxpayer will already be logged into the application (Tax Pro, ECO & DF) and when they click on the “Connect with Us “ button will be sent directly to their eGain Secure Message inbox, where they can view all their messages. eGain Solve Secure Messaging will use Centralized Authorization File (CAF) Power of Attorney Authorization Automation. This project aims to automate the handling of Power of Attorney (POA) or Taxpayer specific authorizations, which are received via Forms 2848 and 8821 and processed manually. These forms are received digitally via eFax and the online portal or through traditional mail. Once received, they must be manually verified by a Tax Examiner to ensure they are complete before being noted on the taxpayer's account. The primary purpose of this automation is to improve time efficiency by reducing manual processing of Forms 2848 and 8821.

Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

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.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address

Agency Sensitive Information

Centralized Authorization File (CAF)

Email Address

Employer Identification Number

Employment Information

Federal Tax Information (FTI)

Financial Account Number

Individual Taxpayer Identification Number (ITIN)

Internet Protocol Address (IP Address)

Name

Other

Protected Information

Social Security Number (including masked or last four digits)

Standard Employee Identifier (SEID)

Tax ID Number

Telephone Numbers

Vehicle Identification Number (VIN)

Please explain the other type(s) of PII that this project uses.

Date of Birth, Place of Birth, Certificate or License Numbers. 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/FTI (including SSN if relevant).

PII for federal tax administration - generally IRC Sections 6001 6011 or 6012

SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of the Inflation Reduction Act (IRA)?

No

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

System

3 What Tier designation has been applied to your system?

1

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

1622

4.12 What is the previous PCLIA title (system name)?

eGain Solve Secure Message, eGain SM

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

To document eGain Solve Secure Messaging's use of Centralized Authorization File (CAF) Power of Attorney Authorization Automation as outlined in PCLIA#1697, Centralized Authorization File (CAF) Power of Attorney Authorization Automation. This project aims to automate the handling of Power of Attorney (POA) or Taxpayer specific authorizations, which are received via Forms 2848 and 8821 and processed manually. These forms are received digitally via eFax and the online portal or through traditional mail. Once received, they must be manually verified by a Tax Examiner to ensure they are complete before being noted on the taxpayer's account. The primary purpose of this automation is to improve time efficiency by reducing manual processing of Forms 2848 and 8821.

5 Is this system considered a child system/application to another (parent) system?

Yes

5.1 Identify the parent system's approved PCLIA number.

1121

5.2 Identify the parent system's name as previously approved.

eGain Solve-Chat-External

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

Yes

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

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

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

The ABA Application ID number is identified as 211458 on the ABA.

10 If this system discloses any PII to any third party outside the IRS, 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?

Yes

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

Yes

12.1 Please identify the Cloud Service Provider (CSP), FedRAMP Package ID, and date of FedRAMP authorization.

Amazon Web Services (AWS) GovCloud, F1603047866, 6/21/2016 eGain, FR2023601671, 12/15/2021

12.2 Does the CSP allow auditing?

Yes

12.21 Who has access to the CSP audit data (IRS or 3rd party)?

IRS

12.3 Please indicate the background check level required for the CSP (None, Low, Moderate or High).

Moderate

13 Does this system/application interact with the public?

Yes

13.1 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

Yes

13.11 Please upload the approved DIRA report using the Attachments button. Select "Yes" to indicate that you have or will upload the signed DIRA form.

Yes

13.2 If individuals do not have the opportunity to give consent to collect their information for a particular use, why not?

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 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.

13.3 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

N/A. The information is collected voluntarily from the taxpayer.

13.4 If information is collected from third-party sources instead of the individual, please explain your decision.

N/A

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

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).

15 Is this system owned and/or operated by a contractor?

Yes, the system is IRS Owned and Contractor Operated

15.1 If a contractor owns or operates the system, does the contractor use subcontractors; or do you require multiple contractors to operate, test, and/or maintain this system?

No

15.2 What PII/SBU data does the subcontractor(s) have access to?

Subcontractors do not have access to the system.

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

IRS Employees: Users and Managers have Read and Write Access; System Administrators have Administrator Access. Contractors: Contractor Users have Read and Write Access; Contractor System Administrators have Administrator Access. Background Investigations are complete for Contractors.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

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

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

Under 50,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Under 5,000

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

More than 1,000,000

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

Not Applicable

22 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.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

Yes

24 Explain any privacy and civil liberties risks related to privacy controls.

There are internal programming consistency checks and record counts to validate the data that is loaded into the system is accurate. All Current eGain Secure Messaging DIRAs have been attached to PCLIA. C-ASCA performed 4/2/2024 listed POA&M 46816, extension date is 12/31/2025.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

Yes

26 Describe this system's audit trail in detail. Provide supporting documents.

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.

27 Does this system use or plan to use SBU data in a non-production environment?

No

Interfaces

Interface Type

IRS Systems, file, or database

Agency Name

Issue Management System (IMS)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Security Audit and Analysis System (SAAS)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

WebApps Enterprise Services, WAES (aka Online Account)

Incoming/Outgoing

Both

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Automated Underreporter (AUR)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Direct File

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

F1120S, Income Tax Return for an S Corporation, related forms & schedules

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

TaxPro

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

RAAS Compliance Data Warehouse (CDW)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

Form 8821 Tax Information Authorization

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Secured channel via HTTPS

Interface Type

Forms

Agency Name

CP2501, Initial Contact - Potential Discrepancy of Income, Deductions and/or Credits Claimed on BMF

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

Form 2848 Power of Attorney and Declaration of Representative

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Secured channel via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

Secure Access Digital Identity (SADI)

Incoming/Outgoing

Both

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

F1065, Return of Partnership Income, related forms & schedules

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

Form 433F, Collection Information Statement

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

CP 2000, Initial Notice - Request Verification for Unreported Income, Deductions, Payments and/or Cr

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

Any tax computation form used in IMF & BMF

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

F1120, Corporate Income Tax Return, related forms & schedules

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Appeals Centralized Database System (ACDS)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Clean Energy Portal

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

Various forms by Collection

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Centralized Authorization File (CAF)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Secured channel via HTTPS

Interface Type

IRS Systems, file, or database

Agency Name

Reporting Compliance Case Management System (RCCMS)

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

Correspondence Examination Automation Support (CEAS)

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

Forms

Agency Name

F1040, Individual Tax Return, related forms & schedules

Incoming/Outgoing

Incoming (Receiving)

Agency Agreement

No

Transfer Method

Amazon Web Services Platform (AWS)

Interface Type

IRS Systems, file, or database

Agency Name

SPLUNK

Incoming/Outgoing

Outgoing (Sending)

Agency Agreement

No

Transfer Method

Secure Data Transfer (SDT)

Systems of Records Notices (SORNs)

SORN Number & Name

IRS 00.001 - Correspondence Files and Correspondence Control Files

Describe the IRS use and relevance of this SORN.

Correspondence received and sent with respect to matters under the jurisdiction of the IRS. Correspondence includes letters, telegrams, memoranda of telephone calls, email, and other forms of communication.

SORN Number & Name

IRS 42.001 - Examination Administrative Files

Describe the IRS use and relevance of this SORN.

eGain Secure Message is used to communicate with taxpayers who are being considered for examination, or who are, or were, examined to determine an income, estate and gift, excise, or employment tax liability. This system consists of investigatory materials required in making a tax determination or other verification in the administration of tax laws and all other sub-files related to the processing of the tax case. This system also includes other management information related to a case and used for tax administration purposes, including classification and scheduling records.

SORN Number & Name

IRS 50.222 - Tax Exempt/Government Entities (TE/GE) Case Management Records

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used to communicate with individuals who are the subject of or are connected to TE/GE examinations and tax determinations, including compliance projects, regarding Federal tax exemption requirements, employee plan requirements, and employment tax requirements. This system consists of records include case identification, assignment, and status information from TE/GE examination and tax determination files, information about individuals pertaining to TE/GE “™s methods of investigating exempt organizations, retirement plans, and government entities with regard to their compliance with statutory Federal requirements and/or their tax-exempt status. In addition, this system contains identifying information regarding informants who have provided information that is significant and relevant to TE/GE investigations of taxpayers.

SORN Number & Name

IRS 26.012 - Offer in Compromise Files

Describe the IRS use and relevance of this SORN.

Taxpayer name, address, Taxpayer Identification Number (TIN) (e.g., Social Security Number (SSN), Employer Identification Number (EIN), or similar number assigned by the IRS),

assignment information; and records, reports and work papers relating to the assignment, investigation, review and adjudication of the offer.

SORN Number & Name

IRS 26.009 - Lien Files

Describe the IRS use and relevance of this SORN.

Open and closed Federal tax liens, including Certificates of Discharge of Property from Federal Tax Lien; Certificates of Subordination; Certificates of Non-Attachment; Exercise of Government “™s Right of Redemption of Seized Property; and Releases of Government “™s Right of Redemption.

SORN Number & Name

IRS 36.003 - General Personnel and Payroll Records

Describe the IRS use and relevance of this SORN.

This system consists of a wide variety of records relating to personnel actions and determinations made about an individual while employed in the Federal service, including information required by the Office of Personnel Management (OPM) and maintained in the Official Personnel File (OPF) or Employee Personnel File (EPF). Information is also maintained electronically in Automated Labor and Employee Relations Tracking System (ALERTS) and Totally Automated Personnel System (TAPS). Listing of employee pseudonyms and Forms 3081 is also included. This system also includes personnel and payroll records (e.g., office/building security records, disciplinary action records, travel/ moving expense records, insurance/ beneficiary records, personal addresses, personal telephone numbers, personal email addresses, emergency contact information, payroll deduction records).

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used to communicate with individuals who file Federal Individual Income Tax Returns; individuals who file other information filings; and individuals operating under powers of attorney. This system consists of Tax records for each

applicable tax period or year, representative authorization information (including Centralized Authorization Files (CAF)), Device ID and a code identifying taxpayers who threatened or assaulted IRS employees. An indicator will be added to any taxpayer "™s account if a state reports to IRS that the taxpayer owes past due child and/or spousal support payments.

SORN Number & Name

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

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used by IRS Customer Service Agents and Revenue Officers working Trust Fund Recovery cases and One Hundred Percent Penalty cases. This SORN covers individuals against whom Federal tax assessments have been made or are being considered as a result of their being deemed responsible for payment of unpaid corporation withholding taxes and social security contributions. This system consists of the following records: Taxpayer name, address, Taxpayer Identification Number (TIN) (e.g., Social Security Number (SSN), Employer Identification Number (EIN), or similar number assigned by the IRS), information about basis of assessment, including class of tax, period, dollar figures, waivers extending the period for asserting the penalty (if any), and correspondence.

SORN Number & Name

IRS 24.047 - Audit Underreporter Case Files

Describe the IRS use and relevance of this SORN.

ROUTINE USES: Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted.

SORN Number & Name

IRS 00.003 - Taxpayer Advocate Service and Customer Feedback and Survey Records

Describe the IRS use and relevance of this SORN.

Individuals who provide feedback (both complaints and compliments) about IRS employees, including customer responses to surveys from IRS business units and IRS employees about whom complaints and compliments are received by the Taxpayer Advocate Service. Quality review and tracking information, customer feedback, and reports on current and former IRS employees and the resolution of that feedback.

SORN Number & Name

IRS 44.003 - Appeals Centralized Data

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used to communicate with taxpayers who seek administrative review of IRS proposed adjustments and collection actions with which they disagree. Individuals who seek administrative review of initial Freedom of Information Act (FOIA) determinations. This system consists of records including information from 24.030, 24.046, 42.001, and 44.001 systems, related internal management information, including the taxpayer "™s DIF Score, and a code identifying taxpayers that threatened or assaulted IRS employees. Information pertaining to FOIA cases under administrative appeal.

SORN Number & Name

IRS 44.001 - Appeals Case Files

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used to communicate with taxpayers who seek administrative review of IRS proposed adjustments and collection actions with which they disagree. Persons who seek administrative review of initial Freedom of Information Act (FOIA) determinations. Records in this system consist of investigatory materials required in making a tax determination or other verification in the administration of tax laws and all other sub-files related to the processing of the tax case, including history notes and work papers required in an administrative review of an assessment or other initial tax determination, collection action, or FOIA determination. This system also includes other management information related to a case.

SORN Number & Name

Treasury .015 - General Information Technology Access Account Records

Describe the IRS use and relevance of this SORN.

This SORN covers all persons who are authorized to access Treasury information technology resources (either directly or via contractor-provided validation services), including employees, contractors, grantees, fiscal agents, financial agents, interns, detailees, members of the public, and any lawfully designated representative of the above as well as representatives of federal, state, territorial, tribal, local, international, or foreign government agencies or entities, in furtherance of the Treasury mission. Individuals who serve on Treasury boards and committees; Individuals who provide personal information to Treasury or a Treasury contractor to facilitate access to Treasury information technology resources; Industry points-of-contact providing business contact information for conducting business with government agencies; Industry points-of-contact emergency contact information in case of an injury or medical notification; Individuals who voluntarily join a Treasury-owned and operated web portal for collaboration purposes; and Individuals who request access but are denied, or who have had their access to Treasury information systems revoked. This system consists of the following records: Driver's License Numbers; Photographs; Universally Unique Identifier (UUID) or other assigned identifier; Social Security number; Business name; Job title; Business contact information; Personal contact information; Pager numbers; Others phone numbers or contact information provided by individuals while on travel or otherwise away from the office or home; Citizenship; Level of access; Home addresses; Business addresses; Personal and business electronic mail addresses of senders and recipients; Justification for access to Treasury computers, networks, or systems; Verification of training requirements or other prerequisite requirements for access to Treasury computers, networks, or systems.

SORN Number & Name

IRS 24.046 - Customer Account Data Engine Business Master File

Describe the IRS use and relevance of this SORN.

Tax records for each applicable tax year or period, including employment tax returns, partnership returns, excise tax returns, retirement and employee plan returns, wagering returns, estate tax

returns; information returns; representative authorization information; and Device ID.

SORN Number & Name

IRS 26.020 - Taxpayer Delinquency Investigation Files

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used to communicate with individuals who are, or may be, delinquent in filing Federal tax returns. The system consists of records including Taxpayer name, Taxpayer Identification Number (TIN) (e.g., Social Security Number (SSN), Employer Identification Number (EIN), or similar number assigned by the IRS); information from previously filed returns, information about the potential delinquent return(s), including class of tax, chronological investigative history; and a code identifying taxpayers that threatened or assaulted IRS employees.

SORN Number & Name

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

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used to communicate with requesters of letter rulings and determination letters, and subjects of field office requests for technical advice and assistance and other correspondence, including correspondence associated with section 527 organizations. Records in this system include Name, date, nature and subject of an assignment, and work history. Subsystems include case files and section 527 records that contain the correspondence, internal memoranda, digests of issues involved in proposed revenue rulings, and related material.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging may be used by individuals who have accessed, by any means, information contained within IRS electronic or paper records or who have otherwise used any IRS computing equipment/resources, including access to Internet sites; individuals whose information is accessed using IRS computing equipment/resources; and IRS employees and contractors who use

IRS equipment to end electronic communications. The system consists of records concerning the use of IRS computing equipment or other resources by employees, contractors, or other individuals to access IRS information; records concerning individuals whose information was accessed using IRS computing equipment/resources; records identifying what information accessed; records concerned the use of IRS computer equipment and other resources to send electronic communications; and records concerning the investigation of such incidents.

SORN Number & Name

IRS 42.021 - Compliance Programs and Projects Files

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used to communicate with individuals covered by this SORN. This includes individuals who may be involved in tax evasion schemes or noncompliance schemes, including but not limited to withholding noncompliance or other areas of noncompliance grouped by industry, occupation, or financial transactions; individuals who may be selling or promoting abusive tax schemes or abusive tax avoidance transactions; individuals who may be in noncompliance with tax laws concerning tax exempt organizations, return preparers, corporate kickbacks, or questionable Forms W ““4, tax evasion schemes involving identity theft, among others. This system consists of records pertaining to individuals in compliance projects and programs, and records used to consider individuals for selection in these compliance projects and programs.

SORN Number & Name

IRS 26.019 - Taxpayer Delinquent Account Files

Describe the IRS use and relevance of this SORN.

eGain Secure Messaging is used to communicate with individuals on whom Federal tax assessments have been made and persons who owe child support obligations. The system consists of investigatory records generated or received in the collection of Federal taxes and all other related sub-files related to the processing of the tax case. This system also includes other management information related to a case and used for tax administration purposes including the Debtor Master File, and records that have a code identifying taxpayers that threatened or assaulted IRS employees.

SORN Number & Name

IRS 00.002 - Correspondence Files: Inquiries about Enforcement Activities

Describe the IRS use and relevance of this SORN.

Taxpayer name, address, and, if applicable, Taxpayer Identification Number (TIN) (e.g., Social Security Number (SSN), Employer Identification Number (EIN), or similar number assigned by the IRS); chronological investigative history; other information relative to the conduct of the case; and/ or the taxpayer "™s compliance history. Correspondence may include letters, telegrams, memoranda of telephone calls, email, and other forms of communication.

SORN Number & Name

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

Describe the IRS use and relevance of this SORN.

ROUTINE USES: OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES: Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103 and 6104 where applicable. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted. To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. EGain Secure Messaging is used to communicate with individuals who submit letter ruling requests or determination letter requests with respect to organizations, or who are the subjects of technical advice requests, where the matter raised has some significance to tax administration. The system consists of the following records: summaries of significant

technical matters pertaining to letter rulings or determination letters under the jurisdiction of the Division Commissioner, TE/GE.

Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

5.2 Transitory and Intermediary Records

What is the GRS/RCS Item Number?

020

What type of Records is this for?

Electronic

Please provide a brief description of the chosen GRS or RCS item.

Intermediary records. Records that meet the following conditions: • They exist for the sole purpose of creating a subsequent record and • They are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. This includes certain analog and electronic source records for electronic systems that are not otherwise excluded. For specific examples, see the GRS 5.2 Frequently Asked Questions (FAQs). Exclusion: Source records that have been digitized. GRS 4.5, item 010, covers these records. Note: The GRS provides disposition authority for copies of electronic records from one system that are used as source records to another system, for example an extracted data set. The GRS does not apply to either the originating system or the final system in which the final records reside. These systems must be disposed of per an agency-specific schedule, or if appropriate, another GRS. It is possible that sometimes information is moved from one system to another without the creation of an intermediary copy.

What is the disposition schedule?

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.

Data Locations

What type of site is this?

System

What is the name of the System?

SPLUNK

What is the sensitivity of the System?

Sensitive But Unclassified (SBU)

What is the URL of the item, if applicable?

Not applicable

Please provide a brief description of the System.

Splunk is a Security Information and Event Management (SIEM) software solution tool composed of various dashboards that IRS employees are using to aggregate and/or analyze security data for systems/applications.

What are the incoming connections to this System?

A data extraction is performed as per National Institute of Standard Technology controls.

What are the outgoing connections from this System?

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.