Date of Approval: 05/01/2025
Questionnaire Number: 2205

Basic Information/Executive Summary

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

Task Request and Case Management System

Acronym:

TRACMS

Business Unit

Privacy, Governmental Liaison and Disclosure

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 Sponsor

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) Office of Governmental Liaison, Disclosure and Safeguards (GLDS) has responsibility for the management of requests for documents pursuant to the Freedom of Information Act (FOIA) and the Privacy Act (PA) and disclosure of tax records under the provisions of Internal Revenue Code (IRC) Section 6103, as well as the responsibility for the activities of the Safeguards programs. GLDS processes approximately 60,000 plus record requests annually. All federal agencies, including the IRS, are required under the FOIA to disclose records requested by any person (minus certain exemptions or exclusions). The Task Request and Case Management system (TRACMS) system was developed to assist the IRS in managing both the workload and the data involved in complying with this act. The GLDS functions are in geographically dispersed offices throughout the USA. The software is customized to meet all

GLDS business requirements (and data capture) for processing disclosure casework under IRC 6103, FOIA, and to comply with the PA. This IRS Cloud web based application allows them to electronically receive and process 6103, FOIA, and PA requests; manage inventory; track Disclosure, Governmental Liaison, Privacy Policy and Knowledge Management (PP&KM), and Safeguards program work activities: maintain the system and document repository to store and retain program records in a cloud-based environment; contain an online request portal for users and evenly distribute workload nationwide, including daily time tracking. The software is customized to meet all GLDS business requirements (and data capture) for processing disclosure casework under Internal IRC 6103, FOIA, and to comply with the PA. We have identified requirements for a cloud web-based system to allow the IRS to fulfill requests with greater efficiency, greater consistency and quality of service to our customers and to be incompliance with known and foreseen changes in law. For example, the Open Government Act (2007) requires updated reporting, the FOIA Improvement Act (2016) mandates a unified records request portal that allows members of the public to submit a request for records, and the Federal Cloud Strategy (2011) urges agencies to consider cloud computing in budgeting. This system currently houses Disclosure casework (for FOIA and other case types), PP&KM, and much of Data Services daily work. The purpose of this cloud web based, software as a service (SaaS) system that, with some modification, replaced the system functionality of the expired AFOIA system and includes all requirements necessary for the addition of Safeguards daily work so that all GLDS functions now use a common electronic solution. GLDS- Data Services (DS) owns and administers TRACMS applications and the cloud contractor service provider. Access to the data is controlled by DS administrators and stored in the cloud database.

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).

Records are maintained in accordance with the Records Control Schedule (RCS)Document 12990 and General Records Schedule (GRS) Document 12829. Four retentions scheduled are set within the TRACMS system. Retention policy is based off case type and last action. (in accordance with the RCS/GRS retention schedule). SBU Data is used as required to determine proper response/ entitlement to response records in accordance with the Freedom of Information Act (FOIA)and IRC 6103.

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

Address

Federal Tax Information (FTI)

Name

Social Security Number (including masked or last four digits)

Standard Employee Identifier (SEID)

Tax ID Number

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

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

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?

No

1.1 What is the name of the Business Unit (BU) or Agency initiative?

Internal Revenue Service (IRS) Office of Governmental Liaison, Disclosure and Safeguards (GLDS)

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

System with applications

3 What Tier designation has been applied to your system?

0

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?

1739

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

GLDS Task Request and Case Management System (TRACMS)

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.)

We have a current PCLIA #1739 but after the Annual Cyber Assessment & Privacy Assessment a recommendation was made to update PCLIA #1739 and complete changes to the PII.

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

No

5.1 Identify the parent system's approved PCLIA number.

Not Applicable

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

Not Applicable

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?

No

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

Privacy, Government Liaison, and Disclosure

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.

Yes- TRACMS is on the ABA, ID number 211201

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

10.1 You have indicated that you do not have an "accounting of disclosures" process is in place; please indicate a projected completion date or explain the steps taken to develop your accounting of disclosures process. Note: The Office of Disclosure should be contacted to develop this system's accounting of disclosures process.

No

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

11.1 Describe the business process and purpose of your Artificial Intelligence (AI) and identify what system(s) or business process(es) this AI supports.

Not Applicable

11.2 What is the algorithm or learning method used and what database is training your AI?

Not Applicable

11.3 How is this AI system tested and validated to ensure that the decisions or outputs are reliable (relevant to the input) and performs without biases and drifting? Note: Outputs include, User information, transfer to assistor, reports on dashboard depicting activities.

Not Applicable

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.

Cloud Service Provider (CSP): AINS DBA OPEXUS-eCase FedRAMP Package ID: AGENCYHUDSAAS Date of FedRAMP authorization: 02/21/2014

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).

High

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?

The information collected under the Freedom of Information Act, is required to perform the search of requested records. Individuals do not have the opportunity to decline from providing the required information. The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

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.

The information collected under the Freedom of Information Act, is required to perform the search of requested records. Individuals do not have the opportunity to decline from providing the required information. Also, regarding the Safeguard segment of the application, the information is not collected directly from individuals. The information collected by state/local or federal agencies is obtained via Transcript Delivery System (TDS) and subsequently provided to Safeguards to justify protection of Federal Tax Information (FTI). Notice, consent and due process are provided via TDS and its related tax forms and instructions, and pursuant to 5 USC.

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

All information is collected from first person or authorized representative.

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. Due process is provided pursuant to 5 USC.

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

Yes, 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?

Yes

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

Read and Write - access to TRACMS documents that contain PII/SBU- High Level. The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties. In accordance with Homeland Security Presidential Directive12 (HSPD-12), the Department of the Treasury Security Manual, Chapter II, Section 2, Investigative Requirements for Contractor Personnel describes "investigative requirements for contract employees, subcontractors, experts, and consultants who require staff-like access, wherever the location, to (1)Treasury/bureau-owned or controlled facilities; or (2) work on contracts that involve the design, operation, repair or maintenance of information systems; and/or (3) require access to sensitive but unclassified (SBU) information. "Internal Revenue Manual (IRM) 10.8.1, Information Technology (IT) Security Policy and Guidance, establishes comprehensive, uniform security policies for the IRS. This manual applies to individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate IT systems containing IRS data. Pursuant to Internal Revenue Service Acquisition Policy (IRSAP)clauseIR1052.239-9007, the contractor is required to furnish the Contracting Officer Representative (COR) a list of names (as well as any other requested, supporting information) of new or substitute contractor employees and the IRS locations for which access is requested. A security screening, if determined appropriate by the IRS and in accordance with IRM 10.23.2,Personnel Security, Contractor Investigations, and TD P 15-71, Chapter II, Section 2, will be conducted by IRS for each contractor employee requiring access to IRS' IT systems, or as otherwise deemed appropriate by the COR. Unless otherwise stated in Treasury regulation, the information shall be submitted within five (5) days of contract award and within 24 hours of the date that the identity of a prospective personnel substitution has been confirmed. In addition to the requirements set forth above, the contractor shall also comply with the following IRS clauses: 1. IR1052.204-9003, IRS Security Awareness Training Requirements 2. IR1052.204-9005, Submission of Security Forms and Related Materials 3. IR1052.204-9006, Notification of Change in Contractor Employee Employment Status, Assignment, or Standing 4. IR1052.239-9007, Access, Use or Operation of IRS Information Technology (IT) Systems by Contractors. Contractor support is required for planning, managing, and executing the design, build, test, and deployment phases of the proposed system. As such, the contractor will be expected to finalize business requirements, develop necessary design specifications, modify the application to meet requirements, develop and execute software testing and data validation to ensure quality deliverables, develop and execute a plan for data conversion, provide system documentation for operation and maintenance support, provide assistance as needed with any Federal Information.

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.)

Users (IRS employee) -Read and Write
Managers (IRS employee) -Read and Write
Sys. Administrators (IRS employee) -Administrator
Developers (Contractor employee) Read and Write
Contractor Users (Contractor employee) Read and Write- Background -High
Contractor Managers (Contractor employee) Read and Write- Background -High
Contractor Sys. Admin. (Contractor employee) - Read and Write- Background-High
Contractor Developers (Contractor employee)-Read and Write- Background-High

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.

The information collected under the Freedom of Information Act, is required to perform the search of requested records. Individuals do not have the opportunity to decline from providing the required information. Also, regarding the Safeguard segment of the application, the information is not collected directly from individuals. The information collected by state/local or federal agencies is obtained via Transcript Delivery System (TDS) and subsequently provided to Safeguards to justify protection of Federal Tax Information (FTI). Notice, consent and due process are provided via TDS and its related tax forms and instructions, and pursuant to 5 USC.

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".

5,000 to 10,000

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 10,000

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 IRS systems or applications, the user's manager, or designated official, accesses the Business Entitlement Access Request System (BEARS) application to request access for the new user. The completed BEARS is submitted to the application administration approval group, and then the user is added by their Standard Employee Identification (SEID). 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 work group assignments. Users such as case workers only have access to input data for their work group assignment, run pre-programmed reports and ad hoc queries, and cannot delete data or records or manipulate or physically access the data. Access to the data tables is restricted to the application, system, and database administrators.

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

No

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

There are no privacy and civil liberties risks related to privacy controls.

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.

No

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

TRACMS Information System Security Officer (ISSO) Continuation Monitoring (ConMon) Reports, FOIAXpress SAAS Audit Reviews, FOIAXpress queries SPLUNK

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

No

Interfaces

Interface Type

Other Federal Agencies

Agency Name

FED=Federal

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Secure Data Transfer (SDT)

Interface Type
IRS Systems, file, or database
Agency Name
Transcript Delivery System (TDS)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Mail

Interface Type
IRS Systems, file, or database
Agency Name
Business Master File (BMF)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Mail

Interface Type
IRS Systems, file, or database
Agency Name
Secure Access Digital Identity (SADI)
Incoming/Outgoing
Transfer Method
Other
Other Transfer Method
IAL2 / AAL2 / FAL2

Interface Type
IRS Systems, file, or database
Agency Name
Integrated Data Retrieval System (IDRS)
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Mail

Interface Type
IRS Systems, file, or database
Agency Name
Individual Master File (IMF)
Incoming/Outgoing
Outgoing (Sending)

Transfer Method
Mail

Interface Type
State Agencies
Agency Name
State Local Government Services (SLGS)
Incoming/Outgoing
Outgoing (Sending)
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.
Surveys will be offered to the taxpayer at the end of the Chat. Responses will be used to measure/improve the program.

SORN Number & Name
IRS 34.037 - Audit Trail and Security Records
Describe the IRS use and relevance of this SORN.
To identify and track any unauthorized accesses to sensitive but unclassified information and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy.

SORN Number & Name
IRS 00.008 - Recorded Quality Review Records
Describe the IRS use and relevance of this SORN.
To administer quality review programs at call sites. Information maintained includes questions and other statements from taxpayers or their representatives on recordings. The primary focus of the system is to improve service of, and retrieve information by, the employee and not to focus on the taxpayer.

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

To maintain records of tax returns, return transactions, and authorized taxpayer representatives.

SORN Number & Name

IRS 36.003 - General Personnel and Payroll Records

Describe the IRS use and relevance of this SORN.

To administer personnel and payroll programs.

SORN Number & Name

IRS 24.046 - Customer Account Data Engine Business Master File

Describe the IRS use and relevance of this SORN.

To maintain records of business tax returns, return transactions, and authorized taxpayer representatives.

SORN Number & Name

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

Describe the IRS use and relevance of this SORN.

To track the issuance and loss of identification media used to authenticate IRS employees and to plan for efficient allocation and utilization of space based upon records showing use of IRS facilities.

SORN Number & Name

IRS 22.062 - Electronic Filing Records

Describe the IRS use and relevance of this SORN.

To administer and market electronic filing programs.

SORN Number & Name

IRS 36.001 - Appeals, Grievances and Complaints Records

Describe the IRS use and relevance of this SORN.

To track, and process, employment-related appeals, grievances and complaints.

SORN Number & Name

IRS 48.001 - Disclosure Records

Describe the IRS use and relevance of this SORN.

To track the processing of requests or demands for agency records under applicable laws and regulations concerning the disclosure of official information.

Records Retention

What is the Record Schedule System?
Record Control Schedule (RCS)
What is the retention series title?
Administrative and Organizational Records
What is the GRS/RCS Item Number?
8 item 70
What type of Records is this for?
Both (Paper and Electronic)
Please provide a brief description of the chosen GRS or RCS item.
The records covered by this Scheduled are created and/or accumulated by Governmental Liaison and Disclosure (GLD).
What is the disposition schedule?
1. Copies that have no further administrative value after the recordkeeping copy is made. This includes copies maintained by individuals in personal files, electronic mail directories, or other directory on hard disk or network drives, and copies on shared network drives used only to produce the recordkeeping copy. AUTHORIZED DISPOSITION Destroy/Delete within 180 days (6 months) after the recordkeeping copy has been made or when no longer needed. 2. Copies used for dissemination, revision, or updating that are maintained in addition to the recordkeeping copy. AUTHORIZED DISPOSITION Destroy/Delete when dissemination, revision, or updating is complete.

What is the Record Schedule System?
Record Control Schedule (RCS)
What is the retention series title?
Administrative and Organizational Records
What is the GRS/RCS Item Number?
8 item 55
What type of Records is this for?
Both (Paper and Electronic)
Please provide a brief description of the chosen GRS or RCS item.
The records covered by this Schedule are created and/or accumulated by Governmental Liaison and Disclosure (GLD).
What is the disposition schedule?
A. Paper. AUTHORIZED DISPOSITION Destroy when 2 years old. B. Reserved. See Item 70 in this Schedule.

What is the Record Schedule System?
Record Control Schedule (RCS)
What is the retention series title?
Administrative and Organizational Records

What is the GRS/RCS Item Number?

8 item 53

What type of Records is this for?

Both (Paper and Electronic)

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

The records covered by this Schedule are created and/or accumulated by Governmental Liaison and Disclosure (GLD).

What is the disposition schedule?

1.Paper. a. Granting access to all the requested records. AUTHORIZED DISPOSITION Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later. b. Responding to requests for nonexistent records; to requestors who provide inadequate descriptions; and requests not processed for failure to pay agency reproduction fees or other reasons. (1) Request NOT appealed. AUTHORIZED DISPOSITION Destroy 6 years after final agency action or 3 years after final adjudication by the courts, whichever is later. (2) Request appealed. AUTHORIZED DISPOSITION Destroy as authorized under Case Files - FOIA Appeals (See Item 54 in this Schedule). c. Denying access to all, or part of the records requested. (1) Request NOT appealed. AUTHORIZED DISPOSITION Retire to Records Center when no longer needed for current operations. Destroy 6 years after date of reply. (2) Request appealed. AUTHORIZED DISPOSITION Retire to Records Center when no longer needed for current operations. Destroy as authorized under Case Files - FOIA Appeals (See Item 54 in this Schedule). 2. Reserved. See Item 70 in this Schedule. B. Official Copy of Requested Records. 1. Paper. AUTHORIZED DISPOSITION Dispose of in accordance with approved Service disposition instructions for the related records or with the related FOIA request, whichever is later. 2. Reserved. See Item 70 in this Schedule. C. FOIA Control Files. 1. Registers or Listings. a. Paper. AUTHORIZED DISPOSITION Retire to Records Center when no longer needed for current operation. Destroy 6 years after date of reply. b. Reserved. See Item 70 in this Schedule. 2. Other Files. a. Paper. AUTHORIZED DISPOSITION Retire to Records Center when no longer needed for current operations. Destroy 6 years after final action by the agency or after final adjudication by courts, whichever is later. b. Reserved. See Item 70 in this Schedule.

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Administration and Organizational Records

What is the GRS/RCS Item Number?

8 item 41

What type of Records is this for?

Both (Paper and Electronic)

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

The records covered by this Schedule are created and /or accumulated by Governmental Liaison and Disclosure (GLD).

What is the disposition schedule?

A. Paper. 1. Record copy (maintained by GLD). AUTHORIZED DISPOSITION Destroy 2 years after superseded. 2.All other offices/copies. AUTHORIZED DISPOSITION Destroy when 2 years old.

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Administrative and Organizational Records

What is the GRS/RCS Item Number?

8 item 54

What type of Records is this for?

Both (Paper and Electronic)

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

The records covered by this Schedule are created and/or accumulated by Governmental Liaison and Disclosure (GLD).

What is the disposition schedule?

Note: This record series does NOT include the actual FOIA Appeal. This is handled by another office. A. Correspondence and Supporting Documents. These files EXCLUDE the official file copy of the records under appeal, if filed herein. 1. Paper. AUTHORIZED DISPOSITION Retire to Records Center when no longer needed for current operations, when records occupy at least one cubic foot of space, and when records will remain at the Records Center for at least a year. Destroy 6 years after final determination by the agency; 6 years after the time at which a requestor could file suit; or 3 years after final adjudication by the courts, whichever is later. 2. Reserved. See Item 70 in this Schedule. B. Official File Copy of Records Under Appeal. 1. Paper. AUTHORIZED DISPOSITION Retire to Records Center when no longer needed for current operations, when records occupy at least one cubic foot of space, and when records will remain at the Records Center for at least a year. Destroy in accordance with approved Service disposition instructions for the related records or with the related FOIA request, whichever is later. 2. Electronic Copies. Records in the above series that may have been created using word processing, e-mail, or some other electronic application. AUTHORIZED DISPOSITION See Item 70 of this Schedule

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)

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 more and more 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 type of site is this?

Environment

What is the name of the Environment?

eGain Chat

What is the sensitivity of the Environment?

Federal Tax Information (FTI)

Please provide a brief description of the Environment.

Two-way communication platform between the IRS and the taxpayer to provide information requested and answer inquiries.

What are the incoming connections to this Environment?

Direct Connection from Customer's device (Phone, PC, etc.)

What are the outgoing connections from this Environment?

Direct connection from IRS site behind the firewall.