Date of Approval: 12/16/2025
Questionnaire Number: 2699

Basic Information/Executive Summary

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

Case Management Application (CMAP) SS-8

Acronym:

CMAP SS-8

Business Unit

Small Business and Self Employed

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 Case Management Application (CMAP) SS-8 is the IRS enterprise system used to support the processing of Form SS-8. The system is owned and administered by Small Business/Self-Employed (SBSE), with operational and technical support provided by IRS Information Technology (IT) system administrators and authorized IRS contractors. Program ownership resides within the SS-8 Program Office, which is responsible for business operations, policy oversight, and workload management associated with worker classification determinations.

The CMAP operates in coordination with the e-Trak system, which serves as the IRS's enterprise digital intake, document imaging, and workflow tracking system. The CMAP and e-Trak environments are hosted within IRS-approved secure cloud and enterprise data center environments and operate within the IRS trusted

network boundary. Both systems are protected by IRS cybersecurity controls and are continuously monitored in accordance with federal security, privacy, and records management requirements.

The CMAP and e-Trak integration is required to support the IRS mission of ensuring proper worker classification and accurate employment tax administration. e-Trak is used to receive, scan, index, route, and electronically control incoming SS-8 applications and related correspondence, including paper submissions converted to digital format. Once intake and indexing are completed in e-Trak, SS-8 case data and documentation are associated with the corresponding case in the CMAP for assignment, tracking adjudication, and correspondence generation.

The CMAP benefits the IRS by providing standardized nationwide processing of SS-8 cases, improved workload visibility, enhanced internal controls, reduced processing times, and improved customer service. The integration with e-Trak strengthens document accountability, improves case timeliness, and ensures end-to-end electronic tracking from initial receipt through final determination. Together, CMAP and e-Trak support automated workflow management, secure electronic storage, integrated correspondence, and improved audit readiness.

The CMAP and e-Trak systems process and transmit Sensitive but Unclassified (SBU) and Personally Identifiable Information (PII) submitted in connection with Form SS-8 requests. Data is received through secure IRS intake methods, including electronic submissions and paper documents scanned into e-Trak. Information is transmitted internally between e-Trak, CMAP, and other authorized IRS systems using IRS-approved encrypted network protocols. Outgoing information, including case correspondence and determinations, is transmitted through IRS-approved correspondence systems and secure mailing services. No unrestricted public system-to-system connections are used.

Access to CMAP and e-Trak data is strictly limited to authorized IRS employees, managers, analysts, and approved contractors who have a verified business need to perform SS-8 case processing, document intake, technical review, correspondence issuance, quality review, program oversight, or system administration. Access is controlled through role-based access controls, multi-factor authentication, and IRS identity management systems. Case data and documents are stored within IRS-approved secure databases and cloud repositories that meet all encryption requirements. Data retention is governed by the National Archives and Records Administration (NARA) and IRS records management policies.

The primary purpose of the Case Management Application (CMAP) SS-8 application is to maintain the resolutions and determinations regarding worker classification requests. Worker classification requests are submitted on Form SS-8 to determine the relationship between the firm and the worker or the firm and its workers according to common law to assist the requestor in ensuring the appropriate amount of taxes are withheld either by an individual or by an entity. This usually arises when there is a disagreement between the worker and the firm regarding whether the worker should be treated as an independent contractor or as an employee. This form can be completed and mailed or eFax to the IRS. The

privacy data stored in the SS-8 application includes taxpayer identification numbers (TINs), taxpayers' names, addresses, their contact information, and other miscellaneous information specific to their case which could contain tax data. The SS-8 application does not interface with any other application. The application is not externally accessible to other areas. The SS-8 application only shares data as required by mutual agreement with workload selection. The information is shared through a report generated within the SS-8 application. SS-8 application users access the data within the SS-8 CMAP application system from their workstations. A Business Entitlement Access Request System (BEARS) request must be submitted to obtain access to the SS-8 CMAP application.

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).

The Case Management Application (CMAP) SS-8 system collects sensitive data when individuals, businesses, or third parties file Form SS-8. Sensitive information from Form SS-8 is classified and securely entered the CMAP system. All sensitive data is encrypted and stored in compliance with IRS security protocols. Role-based access and detailed audit trails ensure only authorized personnel can interact with the data. Secure encryption ensures safe transfer of sensitive data, both internally and with external entities. Data is securely destroyed using established methods, with detailed logs and verification of proper disposal. By following these rigorous processes, the IRS ensures that the sensitive data in the CMAP SS-8 system is handled securely and in compliance with legal and regulatory requirements, from the moment of collection until its destruction.

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

Address
Email Address
Employer Identification Number
Employment Information
Federal Tax Information (FTI)
Individual Taxpayer Identification Number (ITIN)
Internet Protocol Address (IP Address)
Name
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)

Tax ID Number
Telephone Numbers

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
PII for personnel administration - 5 USC
SSN for tax returns and return information - IRC section 6109

Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?
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? (Number)
0

4 Is this a new system?
Yes

5 Is this system considered a child system/application to another (parent) system?
No

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.
Readiness

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.
SB/SE Governance Borad/AD Compliance Governance Board

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.

211626

10 Does this system disclose any PII to any third party outside the IRS?

Yes

10.1 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.

Pega Platform, F1306282198 (PCFG), 3/15/2019

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?

No

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

The SS-8 process and procedures are dictated by the Internal Revenue Manual guidelines. IRS policy allows individuals whose data is in the system the opportunity to clarify or dispute negative determinations through the reconsideration process. Information can only be accessed by IRS auditors with a

need to know. Employees with access acquire access through BEARS system approvals.

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

No

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.)

User - Read and Write
Managers - Read and Write
System Administrators - Administrator
Developers - Read-Only

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 Privacy Act Notice on Form SS-8 states the IRS collects SS-8 information under 26 U.S. C. §§ 6001, 6011, 6109, and 6201. It is used to determine whether a worker is classified as an employee or independent contractor for tax purposes. The IRS may share information with the other involved party (worker or employer). Under 26 U.S.C. §6103 (Confidentiality of Taxpayer Information), taxpayer data is generally protected, but certain disclosures are allowed for tax administration.

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".

Not applicable

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".

Not applicable

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".

Under 100,000

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

Access is obtained through the Business Entitlement Access Request System (BEARS). Management determines access based on business need. A potential user must submit a request for access via BEARS to their local management for approval consideration. Users are not permitted access without an approved BEARS request from an authorized management official. Specific permissions

(Read, Write, Modify, Delete, and/or Print) are defined on the BEARS request and set (activated) by the System Administrator prior to the user being allowed access. User privileges and user roles determine the types of data that each user has access to. Users are assigned to specific modules of the application and specific roles within the modules and accounts follow the principle of least privilege which provides them with the least amount of access to PII data that is required to perform their business function after receiving appropriate approval. Additionally, accounts follow the principle of least privilege which provides them with the least amount of access to PII data that is required to perform their business function. Management monitors system access and removes permissions when individuals no longer require access.

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 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.

Data at rest is stored securely at the database layer of the database server. Case Management Application (CMAP) protects data at rest as follows: Case Management Application (CMAP), in accordance with the Internal Revenue Manual (IRM) 10.8.1.5.6, has employed the following due diligence methods for protecting data at rest that resides on the servers: Case Management Application (CMAP) does not utilize any shares or shared drives. Case Management Application (CMAP) enforces least privileges through Role Based Access Controls that limit users to only the data necessary to perform their assigned duties. Case Management Application (CMAP) reports are printed in accordance with business need. Reports are handled appropriately in accordance with organizational policies. Case Management Application (CMAP) has had a risk assessment conducted. Security Assessment Services has completed a Security Impact Analysis as part of the current security assessment & Authorization (SA&A) cycle. The Case Management Application (CMAP) SS-8 is being updated as part of the current SA&A (Security Assessment & Authorization) to reflect the encryption utilized by the application to protect SBU (Sensitive But Unclassified) data. Physical security is an inherited for CMAP (Case Management Application) at an organizational level. Physical security requirements are detailed in the IRS Facility Security Plan. Within our security accreditation, the protection of data at rest is inherited from Security Control (SC) - 28: Protection of Information at Rest. The General Support Systems (GSSs) (Modernization & Information Technology Services) MITS-24, MITS-30 and MITS-32 inherit the

responsibility for ensuring the information system protects the confidentiality and integrity of information at rest.

27 Does this system use or plan to use SBU data in a non-production environment?
No

Interfaces

Interface Type
Forms
Agency Name
SS-8
Incoming/Outgoing
Incoming (Receiving)
Transfer Method
Other
Other Transfer Method
Data is transferred from the form into CMAP system; it's not disseminated to any other agency or system.

Systems of Records Notices (SORNs)

SORN Number & Name
IRS 24.046 - Customer Account Data Engine Business Master File
Describe the IRS use and relevance of this SORN.
CADE BMF is a system of records that contains taxpayer account information, including tax returns, payments, and adjustments. Employment tax and worker classification determinations, which may include SS-8 decisions. Employer and worker data relevant to tax administration and compliance.

SORN Number & Name
IRS 00.001 - Correspondence Files and Correspondence Control Files
Describe the IRS use and relevance of this SORN.
Covers all IRS records and taxpayer information collected for administration. Ensures Privacy Act compliance, restricting the collection, use, and disclosure of personal data. Allows taxpayers to request access to their records and correct any errors. Limits third-party disclosure except in cases authorized by law.

SORN Number & Name

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

Covers tax return information, including working classification determinations.

SORN Number & Name

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

Tracks access to IRS records to protect taxpayer data.

Records Retention

What is the Record Schedule System?

Record Control Schedule (RCS)

What is the retention series title?

Tax Administration - Examination - 23

What is the GRS/RCS Item Number?

Item 61

What type of Records is this for?

Both (Paper and Electronic)

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

Directors in response to taxpayers' requests involving income, profits, estate, gift, employment, and excise tax matters.

What is the disposition schedule?

a) General written determinations (along with background file documents) issued pursuant to a request made after October 30, 1976. AUTHORIZED DISPOSITION Destroy 3 years after aforementioned determinations are opened to public inspection. b) General written determinations (along with background file documents) issued pursuant to a request made before November 1, 1976. AUTHORIZED DISPOSITION Destroy 3 years after aforementioned determinations are opened to public inspection if funds are appropriated before January 20, 1979). Destroy after January 20, 1979, if funds are not appropriated prior to January 20, 1979. c) Written determinations having significant reference value (as determined by the Secretary) along with background file documents. AUTHORIZED DISPOSITION Destroy when 15 years old.

Data Locations

What type of site is this?
System
What is the name of the System?
CMAP (Case Management Application) SS-8
What is the sensitivity of the System?
Federal Tax Information (FTI)
Please provide a brief description of the System.
The Case Management Application (CMAP) system collects sensitive data when individuals, businesses, or third parties file Form SS-8. Platform Common Framework Group (PCFG) streams log data to the IRS SPLUNK (Splunk Enterprise Security Platform) environment via IRS EPZ (Enterprise Platform Zone), including Audit Logs, System Logs, and Monitoring Data. This ensures ongoing monitoring of platform performance and security status. Provides ongoing monitoring of platform performance and security status.
What are the incoming connections to this System?
TCP (Transmission Control Protocol) for port forwarding of logs.

What type of site is this?
System
What is the name of the System?
SPLUNK (Splunk Enterprise Security Platform)
What is the sensitivity of the System?
Federal Tax Information (FTI)
Please provide a brief description of the System.
PCFG (Platform Common Framework Group) streams log data to the IRS Splunk environment via IRS EPZ (Enterprise Platform Zone), including Audit Logs, System Logs, and Monitoring Data. This ensures ongoing monitoring of platform performance and security status. Provides ongoing monitoring of platform performance and security status.
What are the incoming connections to this System?
TCP (Transmission Control Protocol) for port forwarding of logs.