Date of Approval: **June 09, 2021**

PIA ID Number: **6166**

SYSTEM DESCRIPTION

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

Enterprise Case Management - Form 3949-A External, ECM

Is this a new system?

Yes

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

Enterprise Case Management (ECM) Governance Board and the Commissioner's ECM Executive Steering Committee (ESC)

Current ELC (Enterprise Life Cycle) Milestones:

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

System Development/Milestone 4B

Is this a Federal Information Security Management Act (FISMA) reportable system?

Yes

GENERAL BUSINESS PURPOSE

What is the general business purpose of this system? Provide a clear, concise description of the system, application or database, the reason for the system, and the benefits to the IRS to use the information, and how the information will be used.

Enterprise Case Management (ECM) is a business-driven transformation program that will modernize and migrate business processes into an end-to-end enterprise solution (ECM) established in the Amazon Web Services (AWS) Cloud. Legacy and standalone case management systems or components across the IRS will begin decommissioning. Its purpose is to enhance and improve the efficiency and effectiveness of tax-collection services, taxpayer interactions, collaboration between IRS business units, and services rendered to taxpayers, financial institutions and other government agencies. When taxpayers file their taxes, IRS auditors often uncover variances or issues requiring further analysis. These issues

may result in the need to verify a taxpayer's income, conduct an audit, investigate fraud or perform other actions that would not normally be required on properly submitted tax records. As these issues arise, cases are created to document and track case management activities and resolve taxpayer issues and inquiries. These cases are subsequently assigned to IRS auditors within a business unit. ECM is a singular system for processing and storing this information within the IRS, providing restricted access to IRS auditors, taxpayers, financial institutions and other U.S. government agencies via the Internet. That includes a significant amount of Personally Identifiable Information (PII) and Sensitive But Unclassified Information (SBU). Previous PCLIAs covered Tax Exempt/Government Entities (TE/GE) Exempt Organization Correspondence Unit and Wage & Investment Grants Management processes. This PCLIA will cover Equity Diversity & Inclusion (EDI business process and the Human Capital office (HCO) business process. W&I Submission Processing Form 3949A External Referrals. The following services will be included with Release 2. 1. Ability to create, open, or close cases 2. Ability to assign, reassign, transfer a case or routing cases to specific locations based on business rules 3. Ability to refer or review case 4. Ability to upload artifacts, including documents scanned from a device on the internal IRS network 5. Generate user notifications/alerts for end users 6. Ability to access out of the box reporting and ability to create additional reports ECM is a hybrid Cloud system, supported by services offered by other systems existing on IRS premises. In both IRS On-Premise and Cloud environments, the ECM Program has no physical access to any hardware hosting ECM components or providing ECM-related services. Its users will access ECM using their ADFS (Active Directory Federation Services) accounts and PIV (Personal Identity Verification) cards. ECM's On-Premise components include an Application Programming Interface (API) Gateway and Data Access Service. The API Gateway facilitates the interface between ECM's On-Premise and Cloud components. Data Access Services enable legacy applications and legacy case management information to be incorporated into the overall case management solution (ECM), supports data filtering and curation, and provides communications, security and logging services.

PII DETAILS

Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information: or any other type of Sensitive but Unclassified (SBU) information or PII such as information about IRS employees or outside stakeholders?

Yes

Does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN's) or tax identification numbers (i.e. last 4 digits, etc.)?

Yes

What types of tax identification numbers (TIN) apply to this system?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

Delivery of governmental benefits, privileges, and services.

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

The ECM system requires the use of Social Security Numbers or Employer Identification Numbers because no other identifier can be used to uniquely identify a taxpayer or an organization. SSNs are permissible from the Internal Revenue Code (IRS) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. For example, the Grants Management program allows an individual taxpayer to apply for a grant, therefore requiring an individual taxpayer to use their social security number as the tax identifying number.

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

There is currently not a way to eliminate the use of the social security number since it is required for tax reporting purposes. SSNs are currently captured in the Wage & Investment (W&I) Submission Processing Form 3949A taxpayers complete. ECM is reporting this data element, because it will now be captured in ECM.

Employer Identification Number

Other Taxpayer Identification Number

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

Yes

Specify the PII Elements:

Name
Mailing address
Phone Numbers
E-mail Address
Date of Birth
Standard Employee Identifier (SEID)
Alien Number
Financial Account Numbers
Tax Account Information
Centralized Authorization File (CAF)

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

Yes

Specify the types of SBU from the SBU Types List:

Official Use Only (OUO) or Limited Official Use (LOU) Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy.

Proprietary data Business information that does not belong to the IRS.

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

Yes

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

The taxpayer can include anything in a response such as pictures of Form 3949-A. New Data element fields: Date of Birth Occupation Marital Status - Married Marital Status - Single Marital Status - Head of Household Marital Status - Divorced Marital Status - Separated Name of Spouse Website Alleged Violation of Income Tax Law - False Exemption Alleged Violation of Income Tax Law - False Deduction Alleged Violation of Income Tax Law - Multiple Filings Alleged Violation of Income Tax Law - Organized Crime Alleged Violation of Income Tax Law - Unsubstantiated Income Alleged Violation of Income Tax Law - Earned Income Credit Alleged Violation of Income Tax Law - Public/Political Corruption Alleged Violation of Income Tax Law - False/Altered Documents Alleged Violation of Income Tax Law - Unreported Income Alleged Violation of Income Tax Law - Narcotics Income Alleged Violation of Income Tax Law - Kickback Alleged Violation of Income Tax Law - Wagering/Gambling Alleged Violation of Income Tax Law - Failure to Withhold Tax Alleged Violation of Income Tax Law - Failure to File Return Alleged Violation of Income Tax Law - Failure to Pay Tax Alleged Violation of Income Tax Law - Other Additional Information - Are book/records available Additional Information - Do you consider the taxpayer dangerous Additional Information - Banks, Financial Institutions used by taxpayer Your Name Best Time to Call

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

PII about individuals for Bank Secrecy Act compliance 31 USC

Has the authority been verified with the system owner?

Yes

BUSINESS NEEDS AND ACCURACY

Explain the detailed business needs and uses for the SBU/ PII, and how the SBU / PII is limited only to that which is relevant and necessary to meet the mission requirements of the system. If SSNs (or tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

SBU/PII data is used to: Provide foundational capabilities to ensure multiple business processes can be integrated over time. All information is essential. All SBU/PII is used to support case inventory control, inventory monitoring (i.e., by group and case worker), as well as reporting functions. ECM maintains inventory of cases being resolved for the IRS. No data is redundant or unnecessary. In order to establish, track and manage labor and employee relations case inventory on individual employees (including conduct, performance and grievances for IRS employees) unique identifier information is required. IRC 6011(e)(2)(A) mandates the usage of SSN for the employee tax compliance issues.

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

The data received from internal IRS systems is deemed reliable and is validated for accuracy by the system sending the data as described in that system's PCLIA. IRS employees will manually verify the accuracy of information included in the requester's correspondence.

PRIVACY ACT AND SYSTEM OF RECORDS

The Privacy Act requires Federal agencies that maintain a system of records to publish systems of records notices (SORNs) in the Federal Register for records from which information is retrieved by any personal identifier for an individual who is a US citizen or an alien lawfully admitted for permanent residence. The Privacy Act also provides for criminal penalties for intentional noncompliance.

Does your application or this PCLIA system pertain to a group of any record from which information is retrieved by any personal identifier for an individual who is a US citizen, or an alien lawfully admitted for permanent residence? An identifier may be a symbol, voiceprint, SEID, or other personal identifier that is used to retrieve information.

Yes

Identify the Privacy Act SORN(s) that cover these records.

IRS 24.046 Customer Account Data Engine Business Master File

IRS 00.333 Third Party Contact Records

IRS 22.061 Information Return Master File

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 34.021 Personnel Security Investigations

IRS 34.037 Audit Trail and Security Records

IRS 42.001 Examination Administrative Files

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

Official Use Only

INCOMING PII INTERFACES

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

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Automated Background Information System (ABIS)
Current PCLIA: Yes
Approval Date: 3/16/2020
SA&A: Yes
ATO/IATO Date: 5/13/2019

System Name: Tax Check Program (TCP)
Current PCLIA: No
SA&A: No

System Name: Totally Automated Personnel System (TAPS)
Current PCLIA: Yes
Approval Date: 10/6/2020
SA&A: Yes
ATO/IATO Date: 4/29/2019

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

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: Any agency, bureaus, companies, etc. can report information on Form 3949-A
Transmission Method: IRS Document Upload Tool
ISA/MOU: No

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

No

Does the system receive SBU/PII from other sources?

Yes

Identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: Any agencies, bureaus, companies, etc. can report on Form 3949-A
Transmission Method: Uploaded to Document Upload Tool
ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 3949-A
Form Name: Information Referral

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

No

PRIVACY SENSITIVE TECHNOLOGY

Does this system use social media channels?

No

Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, RFID, etc.?

No

Does the system use cloud computing?

Yes

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

Yes

Date Certified.

1/28/2020

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

IRS

What is the background check level required for CSP?

High

Is there a breach/incident plan on file?

Yes

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

Storage
Transmission
Maintenance

Does this system/application interact with the public?

No

INDIVIDUAL NOTICE AND CONSENT

Was/is notice provided to the individual prior to collection of information?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

Form 3949A is an Information Referral form. This form is for informants to pass information to the IRS. After receipt of this form the IRS determines whether or not to investigate in a much later stage outside of ECM.

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

No

Why not?

Form 3949A is an Information Referral form. This form is for informants to pass information to the IRS. After receipt of this form the IRS determines whether or not to investigate in a much later stage outside of ECM.

How does the system or business process ensure 'due process' regarding information access, correction and redress?

Form 3949A is an Information Referral form. This form is for informants to pass information to the IRS. After receipt of this form the IRS determines whether or not to investigate in a much later stage outside of ECM.

INFORMATION PROTECTION

Identify the owner and operator of the system (could be IRS owned and Operated; IRS owned, contractor operated; contractor owned and operated).

IRS Owned and Operated

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

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

Developers: Administrator

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

Access to SBU/PII is determined by the roles of the employee and maintained through BEARS (Business Entitlement Access Request System) formerly known as OL5081 (system access request), which is approved by managers and system administrators. Access in ECM is based on hierarchy, roles and permissions.

RECORDS RETENTION SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) approved a Records Control Schedule (RCS, IRS Document 12990) for the retention and destruction of official agency records stored in this system?

Yes

How long are the records required to be held under the corresponding GRS or RCS, and how are they disposed of? In your response, please provide the GRS or RCS chapter number, the specific item number, and records series title.

All records housed in the ECM system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has National Archives approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under IRM 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedule (RCS)

29, Items 54 and 440 SPEC (Stakeholder Partnerships, Education and Communication) Grant Application Files and Cooperative Agreements, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. The Information Referral Form (form 3949-A) records in the Documentation Upload Tool must be held for 90 days after verification of successful creation/download in accordance with GRS 5.2, item 020 before it is deleted or destroyed. Information Referral records downloaded will be managed in accordance with RCS 23, item 64 (c). Form 3949-A (Information Referral). Forms 3949-A screened and not selected for examination. (Job No. DAA-0058-2013-0007-0001) AUTHORIZED DISPOSITION Destroy 90 days after receipt, or after the determination is made not to select for examination.

SA&A OR ASCA

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

Yes

What date was it completed?

12/11/2020

Describe the system's audit trail.

The system will use Enterprise Security Audit Trails (ESAT). ESAT provides a security auditing tool that allows collection retention and review of Enterprise Security audit events. ECM is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

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

Stored in Rational Collaborative Lifecycle Management (CLM) Solution and SharePoint site

Were all the Privacy Requirements successfully tested?

Yes

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

No

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

IRS CyberSecurity conducted a security assessment in February 2021 to issue the Authority to Operate (ATO) on 2/9/2021. All customer configurable security controls are implemented as intended and documented in the ECM System Security Plan (SSP).

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

No

NUMBER AND CATEGORY OF PII RECORDS

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

IRS Employees: Under 50,000

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: No

CIVIL LIBERTIES

Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

No

Is the system information used to conduct 'data-mining' as defined in the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804?

No

Will this system have the capability to identify, locate, and monitor individuals or groups of people?

Yes

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

ECM will receive system logs, which contains Internet Protocol (IP) Addresses, Email Address and SEID, from IRS Network devices. Audit Logs and Audit Trails will be captured.

Does computer matching occur?

No

ACCOUNTING OF DISCLOSURES

Does the system include or require disclosure of tax or employee information to anyone other than IRS employees in the performance of their duties, or to the person to whom the information pertains or to a 3rd party pursuant to a Power of Attorney, tax or Privacy Act consent?

No