Date of Approval: **April 13, 2021**

PIA ID Number: **5909**

SYSTEM DESCRIPTION

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

Enterprise Case Management, ECM

Is this a new system?

No

Is there a PCLIA for this system?

Yes

What is the full name, acronym and milestone of the most recent PCLIA?

Enterprise Case Management (ECM) #5218; W & I Grants SharePoint site #4228

What is the approval date of the most recent PCLIA?

6/29/2020

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Significant System Management Changes

New Access by IRS employees or Members of the Public

Internal Flow or Collection

Were there other system changes not listed above?

No

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). Tax Exempt/Government Entities (TE/GE) Exempt Organization Correspondence Unit was the first (Release 1) IRS business unit migrated to ECM with approximately 20 TE/GE Users and approximately 150 Wage & Investment Users. The next business process to migrate to ECM is Wage & Investment Grants Management (approximately 60 users (Grants Program Office & Business Administrators) and Ranking Panel Members in a given year). The following services will be included with Release 2. 1. Ability to create, open, or close cases 2. Ability to assign, reassign or transfer a case 3. Ability to refer or review case 4. Ability to upload artifacts, including documents scanned from a device on the internal IRS network 5. Ability to access historical data and legacy case data 6. Ability to translate scanned documents into a readable format 7. Generate user notifications/alerts for end users 8. Ability to access out of the box reporting and ability to create additional reports The participation of continued business units (TEGE and Wage & Investment) is intended to reduce Information Technology (IT) maintenance costs, as AWS will primarily be responsible for maintaining server hardware in the Cloud. Adding additional business units to ECM will also result in more functionality being added to ECM during future releases. Release 2 will also not include any external users, such as taxpayers, financial institutions and other government agencies. 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) SharePoint site which received an approved PIA 4228 in April 2017. This is not an increase in data elements collected; however, 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
Standard Employee Identifier (SEID)
Financial Account Numbers
Employment Information
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:

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

Protected Information Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government.

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.

State Application Identifier number, Data Universal Numbering System (DUNS) a DUN and Bradstreet (DUNS) number, Competition Identification Number, Funding Opportunity Number are captured in the W&I SharePoint site. SSNs are currently captured in the W&I SharePoint site which received an approved PIA 4228 in April 2017. This is not an increase in data elements collected; however, ECM is reporting this data element, because it will now be captured in ECM. Comments (Disposition) (W&I Grants) (Text field) Case Type (W&I Grants) Authorized Representative (W&I Grants) State Assignment (W&I Grants) Tax Compliance Findings (W&I Grants) (Text field) Compliance Determination Comments (W&I Grants) Supporting Documents (W&I Grants) (upload link) Civil Rights Review Findings (W&I Grants) (text field) Increasing e-file Securing additional funding sources Targeting of underserved populations Recruitment of volunteers Retention of volunteers Expansion of collaborative efforts among community organizations (W&I Grants) Primary focus- 10 points maximum (W&I Grants) Secondary focus (10 points maximum) (W&I Grants) Analyst Performing Review (W&I Grants) (Text) Federal Award Identifier Number (FAIN) on Last Administrative Review (W&I Grants) FAIN on Last Treasury Inspector General for Tax Administration (TIGTA) Review (W&I Grants) FAIN on Last Financial Review (W&I Grants) Evaluative Criteria Comments (W&I Grants) % Elderly E-file (W&I Grants) (text input field) Concerns (W&I Grants) (text input field) Evaluative Criteria # 2 Comments (W&I Grants) Evaluative Criteria # 1 Comments(W&I Grants) Measure A-05 Returns Secondary Focus (W&I Grants) Measure A-04 Returns Primary Focus (W&I Grants) Measure A-03 Sites (W&I Grants) Measure A-02 E-File % (W&I Grants) Measure A-01 Returns (W&I Grants) Narrative (W&I Grants) Comments: Tell us why you did or did not award full points (W&I Grants) Payment Management System (PMS) Personal Identification Number (PIN) (W&I Grants) PMS EIN (W&I Grants) PMS Account Number (W&I Grants) Corrective Action Resolution Comments (W&I Grants) Corrective Action Status (W&I Grants) Follow-Up Actions (W&I Grants) Grant Program Office (GPO) Comments (W&I Grants) Contact Representative (W&I Grants) Organization Address (W&I Grants) Page Reference (W&I Grants) Award Amount (W&I Grants) Primary Focus (W&I Grants) Unique Entity ID (UEI) (W&I Grants) Grants.gov Number (W&I Grants) Secondary Focus (W&I Grants) Authorized Representative: Last Name (W&I Grants) Authorized Representative: First Name (W&I Grants) Authorized Representative: Email (W&I Grants) Type of Applicant 2 (W&I Grants) (drop down) Funding Opportunity Title (W&I Grants) Authorized Representative: Title (W&I Grants) Subject to Review By State Executive Order 12372 Process (W&I Grants) Congressional Districts Of: Applicant (W&I Grants) Descriptive Title of Applicant's Project (W&I Grants) Funding Opportunity Number (W&I Grants) Catalog of Federal Domestic Assistance Number (W&I Grants) Name of Federal Agency (W&I Grants) Zip / Postal Code (W&I Grants) Type of Applicant 1 (W&I Grants) State (W&I Grants) City (W&I Grants) Street2 (W&I Grants) Street1 (W&I Grants) Organizational DUNS (W&I Grants) Employer/Taxpayer Identification Number (EIN/TIN) (W&I Grants) Legal Name (W&I Grants) Federal Award Identifier (FAIN) (W&I Grants)

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

PII for personnel administration is 5 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. This PII data is used to identify related tax cases, ability to make adjustments or changes to an entity's account, to authenticate an entity and for generation of correspondence and documents related to the entity. 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.

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

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: Integrated Data Retrieval System (IDRS)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 10/1/2018

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

No

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

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

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

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Enterprise Case Management (ECM)
Current PCLIA: Yes
Approval Date: 6/29/2020
SA&A: Yes
ATO/IATO Date: 10/16/2020

Identify the authority.

Enterprise Case Management (ECM) system - Internal Revenue Code Sections 6001, 6011, 6012e(a); Internal Revenue Code Section 6109; IRC 6103

For what purpose?

Login and SEIDs are for the system's auditing purpose.

Does this system disseminate SBU/PII to other Federal agencies?

No

Does this system disseminate SBU/PII to State and local agencies?

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

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?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

Notice, consent, and due process are provided in the form/instructions filed by the applicant and pursuant to 5 USC.

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

No

Why not?

The IRS has the legal right to ask for information per Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. The regulations state that taxpayers must file a return or statement with IRS for any tax they are liable for. Their response is mandatory under these sections.

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

Taxpayers are contacted to explain discrepancies identified in the program and information. Taxpayers can respond to any negative determination prior to final action. Notice, consent and due process are provided pursuant to 5 USC.

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: Read Write

IRS Contractor Employees

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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.

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 ESAT. Enterprise Security Audit Trails (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 November 2020 to issue the Authority to Operate (ATO) on 12/11/2020. 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: Under 5,000

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