Date of Approval: **May 28, 2021**

PIA ID Number: **6127**

SYSTEM DESCRIPTION

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

ECM - EDI Anti-Harassment and HCO Labor Relations, ECMEDIHCO

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

Operations & Maintenance (i.e. system is currently operational)

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. The following services will be included with Release 3. 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. Generate user notifications/alerts for end users 6. Ability to access out of the box reporting and ability to create additional reports The participation of continued business units (EDI&HCO) is intended to reduce Information Technology (IT) maintenance costs, as Amazon Web Services (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:

Security Background Investigations

Interfaces with external entities that require the SSN

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

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

The SSN is required to receive incoming cases from the Automated Background Investigations System (ABIS) and The Treasury Inspector General for Tax Administration's (TIGTA)Criminal Results Management System (CRMS) system as well as the Employee Tax Compliance cases from the 701 Individual Master File (IMF) Extract.

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

Masking first 5 digits of SSN on display for ALERTS Labor and Employee Relations cases.

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
Place of Birth
Standard Employee Identifier (SEID)
Mother's Maiden Name
Criminal History
Medical Information
Certificate or License Numbers
Financial Account Numbers

Photographic Identifiers
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:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

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.

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.

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

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.

New Data element fields: Case type Case subtype Case category Incident Date Referral Type Other Referral Type Brief Description Sensitive Case Indicator Sensitive Case Reason Claimant SEID Claimant First Name Claimant Middle Initial Claimant Last Name Claimant Grade Claimant Series Claimant Business Unit Claimant Organization Claimant Title Claimant Gender Claimant Address Line 1 Claimant Address Line 2 Claimant City Claimant State Claimant Zip Claimant Work Phone Claimant Mobile Phone Claimant Home Phone Claimant Email Subject SEID Subject First Name Subject Middle Initial Subject Last Name Subject Grade Subject Series Subject Business Unit Subject Organization Subject Title Subject Gender Subject Address Line 1 Subject Address Line 2 Subject City Subject State Subject Zip Subject Work Phone Subject Mobile Phone Subject Home Phone Subject Email Gender Relationship (between Subject and Claimant) Employee Relationship (between Subject and Claimant) Issue short description Date of Issue Issue long description

(Stakeholder) Employee SEID (Stakeholder) Employee First Name (Stakeholder) Employee Middle Initial (Stakeholder) Employee Last Name (Stakeholder) Employee Work Phone (Stakeholder) Employee Address (Stakeholder) Employee City (Stakeholder) Employee State (Stakeholder) Employee Zip (Stakeholder) Employee Email (Stakeholder) Employee Comments (Stakeholder) Manager of Subject SEID (Stakeholder) Manager of Subject First Name (Stakeholder) Manager of Subject Middle Initial (Stakeholder) Manager of Subject Last Name (Stakeholder) Manager of Subject Work Phone (Stakeholder) Manager of Subject Address (Stakeholder) Manager of Subject City (Stakeholder) Manager of Subject State (Stakeholder) Manager of Subject Zip (Stakeholder) Manager of Subject Email (Stakeholder) Manager of Subject Comment (Stakeholder) 2nd-level Manager of Subject SEID (Stakeholder) 2nd-level Manager of Subject First Name (Stakeholder) 2nd-level Manager of Subject Middle Initial (Stakeholder) 2nd-level Manager of Subject Last Name (Stakeholder) 2nd-level Manager of Subject Work Phone (Stakeholder) 2nd-level Manager of Subject Address (Stakeholder) 2nd-level Manager of Subject City (Stakeholder) 2nd-level Manager of Subject State (Stakeholder) 2nd-level Manager of Subject Zip (Stakeholder) 2nd-level Manager of Subject Email (Stakeholder) 2nd-level Manager of Subject Comments (Stakeholder) Inquiry Official SEID (Stakeholder) Inquiry Official First Name (Stakeholder) Inquiry Official Middle Initial (Stakeholder) Inquiry Official Last Name (Stakeholder) Inquiry Official Work Phone (Stakeholder) Inquiry Official Address (Stakeholder) Inquiry Official City (Stakeholder) Inquiry Official State (Stakeholder) Inquiry Official Zip (Stakeholder) Inquiry Official Email (Stakeholder) Inquiry Official Comments (Stakeholder) Deciding Official SEID (Stakeholder) Deciding Official First Name (Stakeholder) Deciding Official Middle Initial (Stakeholder) Deciding Official Last Name (Stakeholder) Deciding Official Work Phone (Stakeholder) Deciding Official Address (Stakeholder) Deciding Official City (Stakeholder) Deciding Official State (Stakeholder) Deciding Official Zip (Stakeholder) Deciding Official Email (Stakeholder) Deciding Official Comments (Stakeholder) NTEU Official SEID (Stakeholder) NTEU Official First Name (Stakeholder) NTEU Official Middle Initial (Stakeholder) NTEU Official Last Name (Stakeholder) NTEU Official Work Phone (Stakeholder) NTEU Official Address (Stakeholder) NTEU Official City (Stakeholder) NTEU Official State (Stakeholder) NTEU Official Zip (Stakeholder) NTEU Official Email (Stakeholder) NTEU Official Comments (Stakeholder) Witness SEID (Stakeholder) Witness First Name (Stakeholder) Witness Middle Initial (Stakeholder) Witness Last Name (Stakeholder) Witness Work Phone (Stakeholder) Witness Address (Stakeholder) Witness City (Stakeholder) Witness State (Stakeholder) Witness Zip (Stakeholder) Witness Email (Stakeholder) Witness Comments (Stakeholder) Other Type (Stakeholder) Other SEID (Stakeholder) Other First Name (Stakeholder) Other Middle Initial (Stakeholder) Other Last Name (Stakeholder) Other Work Phone (Stakeholder) Other Address (Stakeholder) Other City (Stakeholder) Other State (Stakeholder) Other Zip (Stakeholder) Other Email (Stakeholder) Other Comments (Stakeholder) Proposing Official SEID (Stakeholder) Proposing Official First Name (Stakeholder) Proposing Official Middle Initial (Stakeholder) Proposing Official Last Name (Stakeholder) Proposing Official Work Phone (Stakeholder) Proposing Official Address (Stakeholder) Proposing Official City (Stakeholder) Proposing Official State (Stakeholder) Proposing Official Zip (Stakeholder) Proposing Official Email (Stakeholder) Proposing Official Comments Interviewer Name Interviewee Name Interview Date Interview Notes Meeting Type Meeting Attendee(s) Meeting Comments Acknowledgement of Allegation Date Initial Summary for BOD Date Case Summary was Sent to BOD BOD Action Type BOD Actions BOD Action Date No Interim Actions Needed Note Review Investigation Findings Date Resulting Action Taken

Date Final Investigation Outcomes Received Type of Recommendation Recommendation Date BOD Decision BOD Response BOD Decision BOD Response Date Date Letter Was Send to Employee Employee Response Was Received Indicator Employee Response Oral Reply Requested Indicator Oral Reply Date Oral Reply Method Oral Reply Attendee(s) Oral Reply Summary 1203 Board Meeting Required Indicator Materials Sent to 1203 Board Date 1203 Board Decision Received Date 1203 Board Decision 1203 Board Mitigation Description Date Final Letter Sent to BOD Final Actions Date Case Referred To Labor Relations Indicator Closure Notes Case Disposition Number of Days Suspended

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

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 34.022 Automated Background Investigations System (ABIS)

IRS 36.001 Appeals, Grievances and Complaints Records

IRS 36.003 General Personnel and Payroll Records

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: Federal Investigative Standards - Tax Check Service (FIS-TCS)
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: Treasury Inspector General for Tax Administration
Transmission Method: EFTU
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?

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: Automated Background Information System (ABIS)
Current PCLIA: Yes
Approval Date: 3/6/2020
SA&A: Yes
ATO/IATO Date: 5/13/2019

Identify the authority.

IRS 34.022 National Background and Investigations Center

For what purpose?

A nightly batch process provides information on closed background investigations cases for general reconciliation purposes, so the agency is not constantly responding to requests for information on an ad hoc basis.

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

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: Treasury Inspector General for Tax Administration
Transmission Method: EFTU
ISA/MOU: No

Identify the authority.

A nightly batch process provides information on closed background investigations cases for general reconciliation purposes, so the agency is not constantly responding to requests for information on an ad hoc basis. IRC 6103(h)(1) provides that disclosures of tax information can be made to Treasury employees with a "need to know" for tax administration purposes.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

DO .311 TIGTA Office of Investigations Files
IRS 34.037 Audit Trail and Security Records

For what purpose?

A weekly database backup is provided back to TIGTA for general auditing purposes, so the agency is not constantly responding to their various requests for information on an ad hoc basis.

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?

The information was gathered as part of the employment process when the employee came on-board. Individuals are notified about the authority to collect the information, whether it's mandatory or voluntary, the purpose, etc. at the time of collection. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions.

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

No

Why not?

The ability to identify individuals is essential to the effective conduct of Labor Relations (LR) activities. Employees agree to this use of their information when they accept employment. 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?

Employees may avail themselves of contractual or statutory appeals concerning any conduct or performance-based actions, including National Treasury Employees (NTEU) grievance/arbitration process, Agency Grievance process, Merit Systems Protection Board appeals, or Equal Employment Opportunity complaint processes. Due process is 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: 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. System combines legacy business use functionality of The Automated Labor and Employee Relations Tracking System (ALERTS) and Employee Tax Compliance (ETC). Data is approved for destruction 5 or 6 years after case closure depending on the nature of the labor/employee case. These instructions are published in GRS 2.3 Item 010-Employee relations programs' administrative records-Destroy when 3 years old, but longer retention is authorized if required for business use. GRS 2.8 Item 010-General ethics program records-Destroy 6 years following the conclusion of an ethics regulatory review, provision of advice to an employee, making a determination regarding outside employment or after such determination is no longer in effect or applicable, or when no longer needed for an active investigation; whichever is later, but longer retention is authorized if required for business use. IRS Records Control Schedule (RCS) Document 12990 under RCS 20, items 118(B)-Delete by degauzing or purging system of case 5 years after cutoff. Human Capital Office (HCO) will ensure data retention compliance with these disposition instructions in the ALERTS system environment. HCO and the Records Office will work together to ensure system updates are reflected in future RCS publication versions.

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: Not Applicable

Members of the Public: Not Applicable

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?

Yes

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? Contact Disclosure to determine if an accounting is required.

Yes