Date of Approval: **August 19, 2022**

PIA ID Number: **7220**

SYSTEM DESCRIPTION

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

Inventory Delivery System, IDS

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?

Inventory Delivery System, IDS, 1965 O&M

What is the approval date of the most recent PCLIA?

12/5/2016

Changes that occurred to require this update:

Expiring PCLIA

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.

Collection Services Branch (CSB) CCB

Current ELC (Enterprise Life Cycle) Milestones:

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

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

No

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.

The Inventory Delivery System (IDS) is one of three collection inventory routing systems along with Taxpayer Delinquent Account (TDA) & Taxpayer Delinquent Investigation (TDI) Analysis. IDS is a systemic batch processing system that uses a Blaze Advisor rules engine and predictive models to route collection cases which have not been resolved during the notice process (After 4th Notice) to the downstream collection functions including Field Collection, Queue, Automated Substitute For Return (ASFR) Collection System, and Automated A6020(b). This rule-based, decision support system enhances existing compliance/collection systems of the IRS by directing tax-delinquent cases to the precise point in the collection process where they can be processed. The batch analysis performed generates the data source once a week from the Taxpayer Information File (TIF) and Corporate Files Online (CFOL) and processes data extraction set-automatically. Data files are received daily via Integrated Data Retrieval System (IDRS). IDS consist of the following components: LOAD - The station where initial taxpayer case data is received from various sources. CASE INIT - Case Initialization station which creates IDS specific data for use by the rules engine. RULE PROCESSING - The station where business rules are applied to determine whether cases are closed, referred to other systems, or assigned to another IRS collection function or process. The business rules are maintained by the Collection Analytics Routing and Selection (CARS) group and the models are maintained by the Strategic Analysis and Modeling (SAM) group in Collection Headquarters.

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:

Another compelling reason for collecting the SSN

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

SSNs are used to identify and review cases to verify the correctness of IDS processing, inventory reporting, and error resolution.

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

None as SSNs are currently the only method for analysts to trace cases from inception, through IDS processing, through final update to the Masterfile system to verify correct processing of IDS business rules and/or for error resolution.

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
Tax Account Information

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

No

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

No

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

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 data is necessary to allow analysts to successfully track and troubleshoot specific cases processing through the IDS and downstream systems. Without access to SSNs and EINs there is no way for employees to follow a single specific case to track it through its entire processing lifecycle from inception, through IDS processing, to final Masterfile update so they can determine where and how errors occurred.

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

IDS requirements specify that data must be refreshed (re-extracted from Integrated Data Retrieval Systems (IDRS) or Corporate Files On-Line (CFOL) via Standardized IDRS Access (SIA) if the data is more than 48 hours old. This ensures that the data is accurate, timely, and complete before beginning analysis. Individual applications may also be programmed to automatically re-request data based on pre-determined criteria. Program requirements include checks and balances. Currently, IDS performs internal testing of each subsystem. IDS performs unit and integration testing on all applications. All data within the application undergo validity and consistency checks as per the specifications. All specifications adhere to security and privacy regulations.

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 26.019   Taxpayer Delinquent Account 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 Collection System (ACS)
Current PCLIA: Yes
Approval Date: 11/19/2018
SA&A: Yes
ATO/IATO Date: 11/20/2018

System Name: Standardized IDRS Access Tier II (SIA)
Current PCLIA: Yes
Approval Date: 2/27/2018
SA&A: No

System Name: Integrated Collection System (ICS)
Current PCLIA: Yes
Approval Date: 5/14/2019
SA&A: Yes
ATO/IATO Date: 2/23/2019

System Name: Automated System for Return
Current PCLIA: Yes
Approval Date: 12/1/2016
SA&A: Yes
ATO/IATO Date: 7/15/2019

System Name: 6020(B)
Current PCLIA: Yes
Approval Date: 8/20/2018
SA&A: Yes
ATO/IATO Date: 7/15/2019

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?

Yes

Please identify the form number and name:

Form Number: 1040
Form Name: U. S. Individual Tax Return

Form Number: 1065
Form Name: U.S. Return of Partnership Income

Form Number: 1120
Form Name: U. S. Corporation Income Tax Return

Form Number: 941
Form Name: Employers Quarterly Federal Tax Return

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: IDRS
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: Yes
ATO/IATO Date: 1/17/2018

System Name: Integrated Collection System (ICS)
Current PCLIA: Yes
Approval Date: 5/14/2019
SA&A: Yes
ATO/IATO Date: 2/23/2019

System Name: Automated Collection System (ACS)
Current PCLIA: Yes
Approval Date: 11/19/2018
SA&A: Yes
ATO/IATO Date: 10/15/2019

System Name: 6020(B)
Current PCLIA: Yes
Approval Date: 8/20/2018
SA&A: Yes
ATO/IATO Date: 7/15/2019

System Name: Standardized IDRS Access Tier II (SIA)
Current PCLIA: Yes
Approval Date: 2/27/2018
SA&A: No

System Name: Automated Substitute for Return (ASFR)
Current PCLIA: Yes
Approval Date: 12/1/2016
SA&A: Yes
ATO/IATO Date: 7/15/2019

Identify the authority.

MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301 and 26 U.S.C. 7801.

For what purpose?

To provide inventory control of delinquent accounts.

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?

No

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 IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice in tax return instructions. When a return is selected for Examination, Collection etc., the taxpayer is sent notice of their rights, such as Privacy Act Notice, Your Appeals Rights and How to Prepare a Protest, Overview of the Appeals Process.

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

Yes

Describe the mechanism by which individuals indicate their consent choice(s):

All individuals have the right to decline to provide information. However, they may be subject to Examination or Deficiency procedures, at which time they are provided applicable notices, such as Your Appeals Rights and How to Prepare a Protest.

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

The IDS 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 appeals process.

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 Only

Managers: Read Only

Developers: Read Only

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

Access to data will be based on the approved security rules determined by individual roles and responsibilities and will be restricted to "need to know." Users will follow established IRS procedures for access using Business Entitlement Access Request System (BEARS) and rules described in Unauthorized Access (UNAX).

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.

Records are dispositioned in accordance with RCS 32, item 28: IDS Inputs: includes IDRS, CFOL and ACS Retention Period: 1 year Dating From: 1 year old or when it is no longer needed for administrative, legal audit or other operational purposes whichever is sooner Data Type: IDS Outputs: includes closing transactions or reassignments via IDRS to the Masterfile Retention Period: 1 year Dating From: 1 year old or when no longer needed for administrative, legal, audit, or other operational purposes whichever is sooner. Data Type: MIS results (Specific taxpayer case results) Retention Period: No Limit Dating From: Completion of the related case Data Type: Self-Monitor Case Reports Retention Period: No Limit Dating From: End of monitoring period Data Type: Self-Monitor Lookup Data Retention Period: 6 months Dating From: Completion of monitoring period Data Type: All other IDS Account Data Retention Period: 1 month Dating From: Date of account completion Data Type: Cross Reference Case Data Retention Period: 1 month Dating From: Date of account completion Data Type: Input files from external sources Retention Period: 3 months Dating From: Date file loaded onto IDS Data Type: Output files to external systems Retention Period: 3 months Dating From: Date file created on IDS Data Type: Error Files Retention Period: 3 months Dating From: Date file created on IDS Data Type: Run Control Files Retention Period: 3 months Dating From: Date file created on IDS Data Type: Audit Trails Retention Period: On-line 1 month; Off-line 7 years Dating From: Date file created on IDS

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?

11/1/2015

Describe the system's audit trail.

Audit Trail Information: TINs, updated address, and date, SEID, TIN Type, file source code (tells the type of account). Operating system or system audit logs are used to monitor system operational status and to verify functions and performance of the system. These logs identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator. These audit events are for the system/OS level only. This application relies on the MITS-24 GSS, which it resides on, for the implementation of this portion of the control.

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)?

Information is stored on a SharePoint that can only be access by approved users

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?

IDS performs internal testing of each subsystem. IDS performs unit and integration testing on all applications. All data within the application undergo validity and consistency checks as per the specifications. All specifications adhere to security and privacy regulations.

SBU DATA USE

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

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

11/21/2019

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

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: More than 1,000,000

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?

No

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