

Date of Approval: **September 17, 2021**

PIA ID Number: **6257**

SYSTEM DESCRIPTION

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

Automated 6020b A6020 (A6020B), A6020B

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?

Automated 6020b A6020 (A6020B), A6020B # 3497 PCLIA

What is the approval date of the most recent PCLIA?

8/31/2018

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.

Internal Revenue Service Enterprise Transition Plan (ETP)

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?

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.

The Automated 6020(b) (A6020B) application facilitates case processing of Business Master File (BMF) taxpayers who do not voluntarily file returns timely (i.e., are past the due date of the return). 6020(b) is a paragraph from the Internal Revenue Code (IRC) that gives IRS the authority to file a tax return for a business when it does not file a required return. This application produces a package containing the appropriate forms (940, 941, 943, or 944) and Letter 1085 and Publication 5, which is sent to the taxpayer.

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.)?

No

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
Standard Employee Identifier (SEID)
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.

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)

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.

The data elements are required to carry out Automated 6020(B) (A6020(b) business purposes of gathering tax information for businesses that have not filed tax returns and creating the missing returns for them. Any information that will help in the computation of an accurate taxpayer return is needed to complete this task. Entity and Power of Attorney (POA) information is needed to mail the proposal. Delinquent tax period and Last Period Satisfied (LPS) information is required for systemic calculation of the proposed liability.

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

Automated 6020(B) (A6020(b) receives data from the weekly Integrated Data Retrieval System (IDRS) load process, which has its own verification process for data accuracy, timeliness, completeness and therefore (b) assumes that the data is accurate, timely, and complete when it is provided by Integrated Data Retrieval System (IDRS) weekly load.

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 24.047 Audit Underreporter Case Files

IRS 26.019 Taxpayer Delinquent Account Files

IRS 34.037 Audit Trail and Security Records

IRS 42.021 Compliance Programs and Projects 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: IDRS (Inventory Data Retrieval System)

Current PCLIA: Yes

Approval Date: 10/1/2018

SA&A: Yes

ATO/IATO Date: 10/14/2020

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: 941

Form Name: Employment Tax

Form Number: 940

Form Name: Employer's QUARTERLY Federal Tax Return

Form Number: 943

Form Name: Employer's Annual Tax Return for Agricultural Employees

Form Number: 944

Form Name: Employer's ANNUAL 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: Generalized Mainline Framework
Current PCLIA: Yes
Approval Date: 11/10/2020
SA&A: No

System Name: Notice Delivery System (NDS)
Current PCLIA: Yes
Approval Date: 8/3/2020
SA&A: Yes
ATO/IATO Date: 11/10/2020

System Name: Standardized IDRS Access Tier 2 (SIATIER2)
Current PCLIA: Yes
Approval Date: 2/27/2018
SA&A: No

Identify the authority.

The IRS Authorizing Official (AO) for Automated 6020(b) (A6020(b)), in accordance with the guidance provided by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), the Department of the Treasury, and the Internal Revenue Service (IRS).

For what purpose?

Tax administration is the purpose. A6020(b) does not directly disseminate to other Federal Agencies. One could consider the letter sent by the program such a dissemination, but the question is being answered no, as this is technically done by NDS, not A6020(b).

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?

Prior to being assigned to A6020B inventory, businesses receive Notice CP 259 which advises the businesses to file a delinquent return or contact the IRS to explain why they are not liable. Notice CP259 advises businesses that a substitute return may be filed if they do

not respond. So, individuals are notified that they may end up in A6020B inventory (this is the SBU collected by A6020B).

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

No

Why not?

Because of due process options outlined below in #19.

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

A6020(b) produces a package containing the appropriate forms (940, 941, 943, and 944) and Letter 1085, which is sent to the taxpayer to inform them of any planned adjustments to their account. After the Letter 1085 package is sent to the taxpayer, no action is taken for a minimum of 45 days. Taxpayers can respond to any negative determination prior to final action. Taxpayers may respond to the findings from the IRS in any of the following ways: Prepare and sign tax returns which the taxpayers believe show their correct tax liability and return to the IRS Mail IRS any additional information taxpayers would like IRS to consider Request a conference. The taxpayers have 45 days from the date of the 1085 letter to respond before the IRS process the tax returns that were prepared in the letter. The taxpayers will then be billed for the amount of tax due, plus any additional penalties and interest.

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 Only

IRS Contractor Employees

Contractor Users: Read Only

Contractor System Administrators: Read Only

Contractor Developers: Read Only

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

Management will determine the access to data by users based on a need to know. However, user access is required to be granted access through the OL5081 process and the user's manager must sign for the user's access. Role based access is in place that has to be approved by management. Contractors have read-only access to A6020(b).

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.

Automated 6020(b) System data containing case data related to business entities delinquent in submitting tax returns in a timely manner is scheduled under National Archives and Records Administration (NARA) Job No. N1-58-11-8. RCS 32 Item 49- Automated 6020(b) System. Cut off 3 years after processing year and transfer external media to off-site storage. Delete/Destroy 3 years after cutoff. Data will be maintained for three years and deleted. Also covered under this schedule are 6060(B) System Inputs: Business entity information received from the IDRS system, Employee Data such as User Standard Employer Identifier (SEID), name, and Audit information will be deleted when no longer needed for business; System Outputs: Taxpayer Delinquency Investigation data will be maintained in accordance with Inventory Delivery System (IDS), and Form 1085 will be maintained in accordance with the Notice Delivery System (NDS); System Documentation: Owner's Manual, User Manual, Data Dictionary, Software Design Description, Software Requirements, et al will be destroyed when superseded or 5 years after the system is terminated, whichever is sooner. These disposition instructions will be published in IRM 1.15.35 when next updated. Also covered by IRS Document 12829, GRS 5.2, item 020 Inputs/Outputs and 3.1, item 051 System Documentation.

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?

5/23/2021

Describe the system's audit trail.

A. Taxpayer: For purposes of this PIA, the 'Taxpayer' refers to a business entity. The following information is maintained: Employer Identification Number (EIN) Name Address Power of Attorney (POA) information Delinquent tax period/s Last Period Satisfied (LPS) information B. Employee Data: User Standard Employer Identifier (SEID) Name C. Audit Trail Information: A6020(b) maintains customized audit trail data tailored to the needs of the business unit. Audit records are generated whenever changes are made to the status codes and stored in a table on the Server database. The customized audit logs maintain the following information for each audit record: The unique identifier of the event EIN History Date Case Status Code Tax Period Status Change Date and Time that the event occurred Last Change Date and Time Wage Code Last Period Satisfied (LPS) Tax Period LPS Amount Credit Amount Assessed Amount D. Other: None. A. IRS: IDRS is used to obtain cases information. The cases are identified by a unique TSIGN which identifies the case as A6020(b). TSIGN cases are Taxpayer Delinquent Account (TDA)/ Taxpayer Delinquency Investigation (TDI) assignment code that is provided by IDRS. This information is obtained via batch loading processes. B. Taxpayer: Taxpayer may contact the IRS to provide updates to the Status Code information pertaining to their case file. C. Employee: User SEID and Name are collected from the employee. D. Other Federal Agencies: No other information is obtained from federal agencies. E. State & Local Agencies: No other information is obtained from state and local agencies. F. Other Third-Party Sources: No other information is obtained from other third-party sources. Yes. The data elements are required to carry out A6020(b) business purposes of gathering tax information for businesses that have not filed tax returns and creating the missing returns for them. Any information that will help in the computation of an accurate taxpayer return is needed to complete this task. Entity and Power of Attorney (POA) information is needed to mail the proposal. Delinquent tax period and LPS information is required for systemic calculation of the proposed liability. IDRS reassigns the T-SIGNED cases to the A6020(b) application through a loading process. The IDRS provides Opening, Closing, and Refresh type record information according to an agreed upon record layout. All Opening records load once the input data has been validated. The IDRS data is checked for the correct format by the input load program before being loaded into the A6020(b) database. The input load program checks to verify that numeric and alphanumeric fields are populated by numeric and alphanumeric entries respectively. These entries are verified for correctness before forwarding for A6020(b) processing. User input to the A6020(b) menus is validated against the expected values. Through A6020(b) specific

modules, users are allowed to update the case status code and/or wage amount of A6020(b) records. A6020(b) employs rules to check the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) to verify that inputs match specified definitions for format and content and pre-screens inputs passed to interpreters to prevent the content from being unintentionally interpreted as commands. No processes are executed when invalid responses are entered.

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)?

All test results from the system test plan are kept in DocIT.

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?

For each A6020(b) program identified to be affected, Project Folder will be reviewed. The following SAT test will be performed and run at an IRS Computing Center. The premise of the test described by this plan is "black box" testing. Black box testing is a strategy that is used to verify that a system performs according to its specifications. The system is treated as a black box. The internal logic and structure of A6020(b) will not be examined, but rather test data and test cases will be developed to test the correctness and completeness of the data from the tables, report, and screen output. An End of Test Status Report will be delivered at the end of the test.

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: 100,000 to 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?

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