

NOTE: The following reflects the information entered in the PIAMS website.

A. SYSTEM DESCRIPTION

Authority: Office of Management Budget (OMB) Memorandum (M) 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 & PVR #10- Privacy Accountability and #21-Privacy Risk Management

Date of Approval: July 21, 2015

PIA ID Number: **1419**

1. What type of system is this? Automated 6020b, A6020b

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, and milestone of the most recent PIA.

Automated 6020(b) - A6020(b)

Next, enter the **date** of the most recent PIA. 7/28/2012 12:00:00 AM

Indicate which of the following changes occurred to require this update (check all that apply).

<u>Yes</u>	Addition of PII
<u>No</u>	Conversions
<u>No</u>	Anonymous to Non-Anonymous
<u>No</u>	Significant System Management Changes
<u>No</u>	Significant Merging with Another System
<u>No</u>	New Access by IRS employees or Members of the Public
<u>No</u>	Addition of Commercial Data / Sources
<u>No</u>	New Interagency Use
<u>No</u>	Internal Flow or Collection

Were there other system changes not listed above? No

3. Check the current ELC (Enterprise Life Cycle) Milestones (select all that apply)

<u>No</u>	Vision & Strategy/Milestone 0
<u>No</u>	Project Initiation/Milestone 1
<u>No</u>	Domain Architecture/Milestone 2
<u>No</u>	Preliminary Design/Milestone 3
<u>No</u>	Detailed Design/Milestone 4A
<u>No</u>	System Development/Milestone 4B
<u>No</u>	System Deployment/Milestone 5
<u>Yes</u>	Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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.

Purpose of the System: A6020(b) is a non-filer program. The A6020(b) application processes Business Master File (BMF) taxpayers who do not voluntarily file returns in a timely manner (past the due date of the return). Internal Revenue Code (IRC) 6020(b) provides the Internal Revenue Service (IRS) the authority to file a tax return for a business when it does not file a required return. A6020(b) produces a package containing the appropriate forms (940, 941, 943, and 944) and Letter 1085, which is sent to the taxpayer. The purpose of A6020(b) is to properly assess the amount on a tax proposal for a particular entity (non-filing business taxpayer) through an automated process as outlined in Internal Revenue Manual (IRM) 5.18.2, Business Returns IRC 6020(b). A6020(b) automatically calculates certain proposals, while others require manual research and data input before the application calculates the proposal. Proposals are generated and adapted for printing and mailing by the Notice Delivery System (NDS), located at the National Print Site. Information, both to and from A6020(b), is transported through the secure Enterprise File Transfer Utility (EFTU) which incorporates SSH Tecita, (FIPS 140-2 validated). A6020(b) utilizes a Microsoft Visual Studio .NET (version 3.5) web environment with a Microsoft SQL 2005 database, programmed in C#. End users interact with the application via Microsoft Internet Explorer (IE), a standard web browser application that is part of the IRS Common Operating Environment (COE) on IRS workstations. All end-user access to the system is web-based. A6020(b) incorporates several automated processes including e-mailing Load Reports, generating files to Standardized IDRS Access (SIA), and running an off-shift run of the load program and reports. The Default Returns process is available in electronic format. A6020(b) relies on the MITS-30 General Support System (GSS). The MITS-30 GSS consists of all IRS servers that provide Windows platform to support numerous IRS business applications in production environment located at all computing centers, campuses, Posts of Duties (PODs), and National Office (NCFB).

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information, any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)? Yes

- 6a. If **yes**, does the system use, collect, receive, display, store, maintain, or disseminate Social Security Numbers (SSN s) or variations of SSN s (i.e. last 4 digits, etc.)? No

If **yes**, check who the SSN (or SSN variation) is collected on.

No On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or variations of SSN s) that apply to this system:

<u>No</u>	Social Security Number (SSN)
<u>No</u>	Employer Identification Number (EIN)
<u>No</u>	Individual Taxpayer Identification Number (ITIN)
<u>No</u>	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
<u>No</u>	Preparer Taxpayer Identification Number (PTIN)

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

- 6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates according to Privacy Requirements? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>	<u>On Primary</u>	<u>On Spouse</u>	<u>On Dependent</u>
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
Yes	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	No	No
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No
No	Live Tax Data	No	No	No

6c. Does this system contain SBU information the system that it uses, collects, receives, displays, stores, maintains, or disseminates? No

6d. Are there other types of SBU/PII used in the system? No

6e. Cite the authority for collecting SBU/PII (including SSN if relevant)

- Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
- No SSN for tax returns and return information is Internal Revenue Code Section 6109
- No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
- No PII for personnel administration is 5 USC
- No PII about individuals for Bank Secrecy Act compliance 31 USC
- No Information by CI for certain money laundering cases may be 18 USC

6f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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 variations) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

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 are needed to mail the proposal. Delinquent tax period and LPS information is required for systemic calculation of the proposed liability

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

A6020(b) receives data from the weekly 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 IDRS weekly load.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

If **yes**, enter the SORN number(s) and the complete the name of the SORN.

SORNS Number

SORNS Name

Treas/IRS 24.046 Business Master File

Treas/IRS 34.037 Audit Trail and Security Records System

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles.

NA

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, cloud, global position system (GPS), biometrics, RFID, etc.? No

15. Does the system use cloud computing? No

16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was/is notice provided to the individual prior to collection of information? No

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?

17b. If **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.
The system uses data entered from tax returns filed by taxpayers. They are notified of such collection by the Privacy Act Notice in the tax return instructions.

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):

18b. If no, why not? Tax returns filed by taxpayers are the source of data input into the system

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

I. INFORMATION PROTECTION

20. 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

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

IRS Employees? Yes

<u>IRS Employees?</u>	<u>Yes/No</u>	<u>Access Level(Read Only/Read Write/Administrator)</u>
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Read-Only

Contractor Employees? No

21a. 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).

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ?

Yes

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and 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. 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.

22b. If **no**, how long are you proposing to retain the records? Please note, if you answered no, you must contact the IRS Records and Information Management Program to initiate records retention scheduling before you dispose of any records in this system.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 4/11/2013 12:00:00 AM

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion?

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

23.1 Describe in detail 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 T-SIGN which identifies the case as A6020(b). T-SIGN 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 are 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) menu 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24c. If **no**, please explain why.

24b. If **yes**, Is the test plan in process or completed: Completed

24.3 If **completed/ or in process**, 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 the Detroit Computing Center (DCC) by John Mishler of CAF/RAF Section. 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.

24b.1. If **completed**, 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.

24b.2. If **completed**, were all the Privacy Requirements successfully tested? Yes

24.2 If **completed**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

K. LIVE DATA TESTING

25. Does this system use, or plan to use Live Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

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

26a. IRS Employees: Not Applicable
26b. Contractors: Not Applicable
26c. Members of the Public: 100,000 to 1,000,000
26d. Other: No

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

27a. If **yes**, explain the First Amendment information being collected and how it is used.

27b. If **yes**, please check all of the following exceptions (any one of which allows the maintenance of such information) that apply:

The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance (as noted in Q17). No

The information maintained is pertinent to and within the scope of an authorized law enforcement activity. (As noted in Q 7) No

There is a statute that expressly authorizes its collection. (Identified in Q6) No

27c. If **yes**, will the First Amendment information be used as the basis to make any adverse determination about an individual's rights, benefits, and/or privileges?

28. Is the system information used to conduct data-mining as defined in the *Implementing the 9/11 Commission Recommendations Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

N. ACCOUNTING OF DISCLOSURES

30. Does the system include or require disclosure of tax or employee information to anyone other than IRS employees or IRS contractors 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

If **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

End of Report
