Date of Approval: **January 16, 2020**

PIA ID Number: **4648**

SYSTEM DESCRIPTION

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

Direct Payment Bonds Database, DPB

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?

Direct Payment Bonds Database

What is the approval date of the most recent PCLIA?

12/16/2016

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.

TEGE Investment Executive Steering Committee IESC

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 general purpose for the Direct Payment Bonds (DPB) database is to record and maintain an accurate account of claimants who request payment. Claimants request credits in lieu of exemption for interest payments, as allowed by the American Recovery and Reinvestment Act (ARRA) 2009 and the Hiring Incentive to Restore Employment Act (HIRE) of 2010. All claimants use Form 8038-CP to request payment of their claimed credits and this form data is entered into the DPB database. Tax Exempt Government Entities (TE/GE) uses this data to create internal reports and identify previously requested credits.

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?

Employer 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

Standard Employee Identifier (SEID)

Tax Account Information

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?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Tax periods

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 EIN of both the payee and issuer is needed for tax identification purposes. Standard Employee Identifier (SEID) is needed to identify the employee who worked the credit request.

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

Data entry is performed by specifically trained individuals. Validation rules are built into the DPB database to ensure accuracy, timeliness and completeness of data. The 8038-CP is rejected if these fields are not validated.

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 50.222 Tax Exempt/Government Entities (TE/GE) Case Management Records

IRS 34.037 Audit Trail and Security Records

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?

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

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

Does the system receive SBU/PII from other sources?

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 8038-CP Form Name: Return for Credit Payments to Issuers of Qualified Bonds

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

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

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?

Notice is provided to individuals by other IRS applications or through forms (e.g., 8038-CP form) that interact directly with the taxpayer at the time of collection. Due process is provided pursuant to Title 5 United States Code (USC).

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):

The IRS has the legal right to ask for information per IRC 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." Any individual employee information is received from a system that provides employees with notice and rights to consent and/or amend, as needed.

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

This database is only a repository of information found on form 8038-CP. This database does not interact with taxpayers directly and thus "due process" is addressed by other IRS applications that directly interact with taxpayers. 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: Read Write

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

The DPB database is located on a secure shared server; each user must obtain permission to access the server folder to be able to use the database. Access to the server folder is approved by management overseeing the DPB requests on a case by case basis. Approved folder access is maintained by Information Technology (IT) through the OS GetServices system.

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 DPB database 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 and Records Administration approval to affect data disposition. Any records generated and maintained by the system will be managed according to requirements under Internal Revenue Manual 1.15.1 and 1.15.6, and will be destroyed using IRS Records Control Schedule 24, Item 92 and as coordinated with the IRS Records and Information Management 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)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

No

Describe the system's audit trail.

The audit trail is maintained by IT and access is granted by requests made through share drive owners who were approved by IT. TE/GE BSP maintains records of individuals who have access to the shared server folder. The DPB database is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

This is an internally created Access database that did not follow an IT or Business Systems Planning (BSP) path in development. The BSP office is now in the process of analyzing the current state and considering options for either improving the existing tool or transitioning to an enterprise solution.

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: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

Direct payment bond claimants (100,000)

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