

Date of Submission: January 10, 2017

PIA ID Number: 1919

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Bank Discrepancy, BANK DISC

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, PIA ID Number and milestone of the most recent PIA.

BANK DISCREPANCY (BANK DISC) ID NUMBER 523

Next, enter the **date** of the most recent PIA. 11/8/2013

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

<u>No</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.

The Bank Discrepancy program is used by Accounting Operations to control and track bank discrepancy inventories. The Bank Discrepancy Application controls and monitors Unresolved Debit Vouchers (Standard Form (SF) 5515) received from depositories which indicate discrepancies between the original Deposit Ticket (SF 215A) and the supporting checks such as: Encoding Errors, Slipped Blocks, piggy back checks, lost checks, and improper SF 5515 charge backs. The federal tax deposits that business owners make to banks to pay their quarterly taxes are not part of the bank discrepancy inventories. The Internal Revenue Service (IRS) deposits all monies paid to IRS by the taxpayer. Discrepancies occur when input errors in depositing the checks are encoded incorrectly. For example: the taxpayer writes a check for \$1,000.00, IRS encodes the check for \$10,000.00 in error. The depository will return the \$9,000.00 debit voucher back to IRS. The Bank Discrepancy Application controls the returned Debit Voucher until the taxpayer is debited for the \$9,000.00 via the Dishonored Check File database. The application controls these cases by systemically assigned sequence numbers for each debit voucher or deposit ticket number entered. History is retained for each case. Baseline or customized reports can be generated for management use. Managers, administrators and account technicians for Bank Discrepancy will have access to the data. This access is determined by the manager based on a user's position and need-to-know. All data is manually input into the system. IRS employees manually research/pull personally identifiable information (PII) data from Integrated Data Retrieval System (IDRS). This is a manual interaction and not systemic one.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or 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 tax identification numbers (i.e. last 4 digits, etc.)? Yes

If **yes**, check who the SSN (or tax identification number) is collected on.

Yes On Primary Yes On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	Social Security Number (SSN)
Yes	Employer Identification Number (EIN)
Yes	Individual Taxpayer Identification Number (ITIN)
Yes	Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
Yes	Practitioner Tax Identification Number (PTIN)

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

The BANK DISC system requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) No

6c. Does this system contain SBU information that is not PII, 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)
Yes	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
Yes	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 tax identification numbers) are used, explicitly explain why use of SSNs meets this criteria. Be specific.

Each data item is required to gather history from time of receipt to closing of each debit voucher (DV) or deposit ticket (DT). The application is a control and tracking system for DV and DT received from the depository.

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

Each DV or DT is balanced prior to being entered on the application, and when assigned on the application. All reports have an indicator that denotes cases that are over 90 days old. An age report can be generated and customized to generate specific age dates.

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.

<u>SORNS Number</u>	<u>SORNS Name</u>
Treas/IRS 24.030	IMF
Treas/IRS 24.046	BMF

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

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? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? No

12b . Does this system disseminate SBU/PII to other Federal agencies? No

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12e. Does this system disseminate SBU/PII to other Sources? 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

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.

This system does not collect directly from individuals because is designed to receive debit voucher (DV) or deposit ticket (DT). The application is a control and tracking system for DV and DT received from the depository.

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

18b. If no, why not? Because the system was designed to receive debit voucher (DV) or deposit ticket (DT). The application is a control and tracking system for DV and DT received from the depository.

19. How does the system or business process ensure due process regarding information access, correction and redress? Not applicable

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

Contractor Employees? No

<u>Contractor Employees?</u>	Yes/No	Access Level	Background Invest. Level
Contractor Users			
Contractor Managers			
Contractor Sys. Admin.			
Contractor Developers			

21a. How is access to SBU/PII determined and by whom? Managers in Campus Accounting Dishonored Check function will approve users via Online 5081. SAs/Managers determine access level for each user.

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 ? No

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.

Bank Discrepancy data is approved for deletion/destruction 6 years, 3 months after the period covered by the account (Job No. N1-58-11-3, approved 6/5/12). These disposition instructions are published in Document 12990 under Records Control Schedule (RCS) 29, item 157. 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, and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer.

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? 12/7/2016

23.1 Describe in detail the system's audit trail. Audit trail records for the transactions identified above includes the following data elements, where applicable: The type of event (e.g., command code), the terminal and employee identification, date and time of input, and account accessed to include the Taxpayer Identification Number (TIN), Master File Tax (MFT), and tax period.

J. PRIVACY TESTING

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

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?

A test plan will also be developed and tested as part of the application's current Annual Security Control Assessment (ASCA) activities. The boundary of the Security Test &Evaluation (ST&E) includes all modules of the BANK DISC application and the BANK DISC application database

24b.1. If **completed**, where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)? The test results are stored in the Treasury FISMA Inventory Management System (TFIMS). The Appendix E, Tier 3 Security Assessment Report (SAR). This appendix documents the risks to the lower tiered system noted above, which may have a separate Authorizing Official than its aligned tier 1 system. The risks have been determined by applying the methodology outlined in Section 2 of the Tier 1's Security Assessment Report (SAR), to the vulnerabilities identified by the security controls assessment. Bank Discrepancy is a Minor Application and its Internal Revenue Service FISMA Inventory Classification is Tier 3.

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. SBU Data Use

25. Does this system use, or plan to use SBU 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: Under 50,000
26b. Contractors: Not Applicable
26c. Members of the Public: Not Applicable
26d. Other: No

M. CIVIL LIBERTIES

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

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 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

End of Report
