Date of Approval: December 4, 2018 PIA ID Number: **3788**

## A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Title 31 Non-Banking Financial Institution Database Title 31, Title 31

2. Is this a new system? No

2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

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

Title 31 Non-Banking Financial Institution Database (# 1582)

Enter the approval **date** of the most recent PCLIA. 02/05/2016

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

No Addition of Personally Identifiable Information (PII) (PII is any information that is linked or linkable).
No Conversions
No Anonymous to Non-Anonymous
Yes Significant System Management Changes
No Significant Merging with Another System
No New Access by IRS employees or Members of the Public
No Addition of Commercial Data / Sources
No New Interagency Use
No Internal Flow or Collection
Yes Expiring PCLIA

Were there other system changes not listed above? No

3. What governance board or Executive Steering Committee (ESC) does this system report to? Full name and acronym.

IT's Compliance Domain ESC

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

No Vision & Strategy/Milestone 0
No Project Initiation/Milestone 1
No Domain Architecture/Milestone 2
No Preliminary Design/Milestone 3
No Detailed Design/Milestone 4A
No System Development/Milestone 4B
No System Deployment/Milestone 5
Yes 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 Title 31 application is an on-line database containing the Non-Bank Financial Institution (NBFI) workload inventory that is defined and governed by the Bank Secrecy Act (BSA). The Title 31 Database provides an inventory management system that allows Bank Secrecy Act (BSA) managers to access cases assigned to their respective groups. The Title 31 contains all the entities identified by BSA as being under IRS jurisdiction for Title 31 compliance. It is used by Small Business and Self-Employed (Operating Division) (SBSE) BSA Exam Case Selection (ECS) Coordinators to deliver examination inventory to the field groups. It is used by the field groups to update information and input examination results. Title 31 Examiners review these cases to determine if any case is not in compliance with financial regulations and make appropriate referrals to the Financial Crime Enforcement Network (FinCEN) and/or Criminal Investigation (CI) for further review. It is also used to provide business results to BSA Management.

**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

6.a. 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 all types of tax identification numbers (TIN) that apply to this system:

| | |
|---|---|
| Yes | Social Security Number (SSN) |
| Yes | Employer Identification Number (EIN) |
| No | Other Taxpayer Identification Number |

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

| | |
|---|---|
| No | Security background investigations |
| No | Interfaces with external entities that require the SSN |
| Yes | Legal/statutory basis (e.g. where collection is expressly required by statute) |
| Yes | When there is no reasonable alternative means for meeting business requirements |
| Yes | Statistical and other research purposes |
| No | Delivery of governmental benefits, privileges, and services |
| No | Law enforcement and intelligence purposes |
| No | Another compelling reason for collecting the SSN |

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

There is a business need for use of SSNs for research abilities. Title 31 Database is not a Taxpayer Identification Number (TIN) based system and is not derived from Title 26 USC income tax data. (Negative TIN Checking) NTIN and Internal Revenue Code (IRC) §6103 does not apply to the Title 31 Application. Title 31 notifies users of their responsibilities to self-report any access that would constitute an Unauthorized Access (UNAX) violation upon entry into the system.

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

Title 31 will continue to truncate the Social Security Number (SSN).

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? Yes

If **yes**, specify the information.

| Selected | PII Element |
|---|---|
| Yes | Name |
| Yes | Mailing address |
| Yes | Phone Numbers |
| No | E-mail Address |
| No | Date of Birth |
| No | Place of Birth |
| Yes | Standard Employee Identifier (SEID) |
| No | Mother's Maiden Name |
| No | Protection Personal Identification Numbers (IP PIN) |
| No | Internet Protocol Address (IP Address) |
| No | Criminal History |
| No | Medical Information |
| No | Certificate or License Numbers |
| No | Vehicle Identifiers |
| No | Passport Number |
| No | Alien Number |
| No | Financial Account Numbers |
| No | Photographic Identifiers |
| No | Biometric Identifiers |
| No | Employment Information |
| No | Tax Account Information |
| No | Centralized Authorization File (CAF) |

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

| Selected | SBU Name | SBU Description |
|---|---|---|
| Yes | Agency Sensitive Information | Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission |
| No | Procurement sensitive data | Contract proposals, bids, etc. |
| No | Official Use Only (OUO) or Limited Official Use (LOU) | Information designated as OUO or LOU is information that: is exempt under one of the statutory Freedom of Information Act exemptions; is prohibited by other laws or regulations; would significantly impede the agency in carrying out a responsibility or function; or would constitute an unwarranted invasion of privacy. |
| No | Proprietary data | Business information that does not belong to the IRS |
| Yes | Protected Information | Information which if modified, destroyed or disclosed in an unauthorized manner could cause: loss of life, loss of property or funds by unlawful means, violation of personal privacy or civil rights, gaining of an unfair procurement advantage by contractors bidding on government contracts, or disclosure of proprietary information entrusted to the Government |

| | | |
|---|---|---|
| No | Physical Security Information | Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities |
| Yes | Criminal Investigation Information | Information concerning IRS criminal investigations or the agents conducting the investigations. |

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

6.e. 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

Yes PII for personnel administration is 5 USC

Yes PII about individuals for Bank Secrecy Act compliance 31 USC

Yes Information by CI for certain money laundering cases may be 18 USC

6.f. 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.

Title 31 will continue to truncate the SSN and Employer Identification Number (EIN). There is a business need for use of SSNs and EINS for research abilities. Title 31 Database is not a TIN based system and is not derived from the Title 26 USC income tax data. NTIN and IRC §6103 does not apply to the Title 31 Application. Title 31 notifies users of their responsibilities to self-report any access that would constitute a UNAX violation upon entry into the system. All items are required for the business purpose of the system. The system is designed to identify, build, and monitor Title 31 examination cases.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

Completeness and accuracy will be verified by managerial review of system generated correspondence and forms, by built in validation rules and record 'normalization' routines, and by matching to commercial locator service databases. Timeliness will be verified by BSA reviewers and coordinators and by managerial review of system generated correspondence.

## C. 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.*

9. 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

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

| SORNS Number | SORNS Name |
|---|---|
| IRS 34.037 | Audit Trail and Security Records |
| IRS 42.031 | Anti-Money Laundering/Bank Secrecy Act and Form 8300 |

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNs please email *Privacy.*

## 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? Yes

11.a. If **yes**, does the system receive SBU/PII from IRS files and databases? Yes

If **yes**, enter the files and databases.

| System Name | Current PCLIA | Approval Date | SA&A? | Authorization Date |
|---|---|---|---|---|
| Criminal Investigation General Support System (CI-1) | Yes | 04/26/2017 | Yes | 03/22/2018 |
| Criminal Investigation Management Information System (CIMIS) | Yes | 05/27/2016 | Yes | 02/05/2013 |

11.b. Does the system receive SBU/PII from other federal agency or agencies? Yes

If **yes**, for each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA)/Memorandum of Understanding (MOU).

| Organization Name | Transmission method | ISA/MOU |
|---|---|---|
| FinCEN | Manual | Yes |

11.c. Does the system receive SBU/PII from State or local agencies? Yes

If **yes**, for each state and local interface identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

| Organization Name | Transmission method | ISA/MOU |
|---|---|---|
| **50 States** | **Manual** | **Yes** |

11.d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

| Organization Name | Transmission method | ISA/MOU |
|---|---|---|
| Internet | Manual | No |

11.e. Does the system receive SBU/PII from **Taxpayer** forms? No

11.f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

## F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

| System Name | Current PCLIA | Approval Date | SA&A? | Authorization Date |
|---|---|---|---|---|
| Criminal Investigation General Support System (CI-1) | Yes | 04/26/2017 | Yes | 03/22/2018 |
| Criminal Investigation Management Information System (CIMIS) | Yes | 05/27/2016 | Yes | 02/05/2013 |

Identify the authority. The BSA, at 31 USC 5319, provides that BSA reports and information are to be made available to governmental entities and certain self-regulatory organizations upon request of the head of the agency or organization. (a). The dissemination must be for the purposes of the BSA described at 31 USC 5311 as criminal, tax, or regulatory investigations or proceedings, or the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism. (b). The head of the agency must make the request in writing, stating the particular information desired and the criminal tax or regulatory purpose for which the information is sought and the official need for the information. 31 CFR 1010.950(c). The Secretary may in his discretion disclose information reported under the BSA for any reason consistent with the purposes of the BSA. 31 CFR 1010.950(a).
For what purpose? All items are required for the business purpose of the system. The system is designed to identify, build, and monitor Title 31 examination cases.

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

12.c. Does this system disseminate SBU/PII to State and local agencies? Yes

If **yes**, identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

| Organization Name | Transmission method | ISA/MOU |
|---|---|---|
| States | Manual | No |

Identify the authority. 31 USC 5311 and 31 USC 5319.

Identify the routine use in the applicable SORN (or Privacy Act exception.) Disclose information to any agency, including any State financial institutions supervisory agency, United States intelligence agency or self-regulatory organization registered with the Securities and Exchange Commission or the Commodity Futures Trading Commission, upon written request of the head of the agency or organization. The records shall be available for a purpose that is consistent with title 31, as required by 31 U.S.C. 5319.

For what purpose? 31 USC 5311 and 31 USC 5319 States: - Many states provide lists of Money Service Business (MSB)s to Bank Secrecy Act (BSA) Management on a quarterly basis. For each state a Memo of Understanding (MOU) between BSA Management and the state's tax Administration offices is in place. The states send current listing of state licensed and supervised MSBs and certain other Non-Banking Financial Institutions (NBFIs), reports of Examination findings of MSBs and certain other NBFIs, correspondence to MSBs and other NBFIs as the information relates to BSA (Title 31) and agent lists, information concerning identified or suspected issues of Title 31 non-compliance, quarterly exam schedule for MSBs, program documents that guide state examiners during the course of MSB and NBFI examinations, and other State and NBFI information - information that is collected in the course of screening, licensing, chartering and examining MSBs and NBFIs.

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

12.e. 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, global position system (GPS), biometrics, Radio Frequency Identification (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 (or is) notice provided to the individual prior to collection of information? No

17.b. 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 Information is not collected directly from an individual. The information is used for law enforcement purposes, collecting the information directly from the individual is not practicable because it would notify them that they are under investigation and may cause them to alter their practices to avoid detection.

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

18.b. If individuals do not have the opportunity to give consent, why not?
The system is a database of Money Service Businesses and is built from third party sources. The data contained is verified during the examination process as outlined in Internal Revenue Manual (IRM) 4.26.9 Examination Techniques for Bank Secrecy Act Industries.

19. How does the system or business process ensure due process regarding information access, correction and redress?
The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is provided pursuant to 5 USC.

## 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

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

Contractor Employees? No

21.a. How is access to SBU/PII determined and by whom? Bank Secrecy Act (BSA) users apply for access to a user specific domain via OnLine-5081 process. During the OnLine-5081 approval process, the BSA functional OnLine-5081 administrator determines appropriateness of user group. There are additional access controls within the user group table within the application. Data access is limited to the approved user group role.

## 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

22.a. 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.

Title 31 data is approved for destruction when 20 years old or when no longer needed for administrative, legal, audit or other operational purposes, whichever is later (Job No. DAA-0058-2012-0007). These data disposition instructions, along with dispositions approved for Title 31 inputs, outputs, system documentation, audit logs and system backups will be published in Document 12990 under Records Control Schedule (RCS) 28, item 242c for Collection when next updated/published.

## I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? Yes

23.a. If **yes**, what date was it completed? 03/22/2018

23.1. Describe in detail the system's audit trail. A complete audit trail of the use of the system is captured and includes every login, logoff, file access and database query. The system monitors for security risks and compliance violations to ensure that the use of the system takes place only for an approved purpose that is within the professional responsibility of each user. Title 31 is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards.

## J. PRIVACY TESTING

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

24.a. If **yes**, was the test plan completed? Yes

If **no**, is the test plan scheduled for completion?

24.a.1. If **yes**, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? Treasury FISMA Inventory Management System (TFIMS)

24.a.2. If **yes**, were all the Privacy Requirements successfully tested? Yes

24.a.3. If **yes**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? No

24.1. Describe what testing and validation activities which have been conducted or are in process to verify and validate that the applicable Privacy Requirements (listed in header) have been met? The Continuous Monitoring and the Security Assessment and Authorization processes ensure that the controls continue to work properly in safeguarding the PII.

## 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:

| | |
|---|---|
| 26.a. IRS Employees: | Under 50,000 |
| 26.b. Contractors: | Not Applicable |
| 26.c. Members of the Public: | 100,000 to 1,000,000 |
| 26.d. 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 Recommendations of the 9/11 Commission 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

30. Does Computer matching occur? No

## N. ACCOUNTING OF DISCLOSURES

31. 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**