Date of Approval: **November 16, 2021**

PIA ID Number: **6487**

SYSTEM DESCRIPTION

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

Title 31 NonBanking Financial Institution Database, T31 NBFI

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?

Title 31 Non-Banking Financial Institution Database (# 3788)

What is the approval date of the most recent PCLIA?

12/8/2018

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.

IT's Compliance Domain Executive Steering Committee (ESC)

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 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 (SBSE) Operating Division, BSA Exam Case Selection (ECS) Managers, and 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.

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?

Social Security Number (SSN)

List the approved Treasury uses of the SSN:

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

There is a business need for use of SSNs to identify trades ad businesses subject to Title 31 regulations. SSNs are not a mandatory requirement for T31 NFBI database. T31 NFBI 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) Â§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)

Employer Identification Number

Other Taxpayer 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
Mailing address
Phone Numbers
Standard Employee Identifier (SEID)
Internet Protocol Address (IP Address)

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.

Proprietary data Business information that does not belong to the IRS.

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.

Criminal Investigation Information Information concerning IRS criminal investigations or the agents conducting the investigations.

Are there other types of SBU/PII used in the system?

No

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

PII about individuals for Bank Secrecy Act compliance 31 USC

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

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.

Title 31 will continue to truncate the SSN and Employer Identification Number (EIN). There is a business need for use of SSNs and EINS to identify trades and businesses subject to the Title 31 regulations. Title 31 Database is not a TIN based system and is not derived from the Title 26 USC income tax data. NTIN and IRC Â§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. The use of this PII along with the taxpayers' name, mailing address, phone numbers and Employees SEIDs are used to deliver examination inventory to the field groups. It allows the field groups to update pertinent information, input examination results, and track referrals to the Financial Crime Enforcement Network (FinCEN) and/or Criminal Investigation (CI).

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

Case coordinators verify SBU/PII data for accuracy by matching it to public records and asset locator service databases such as Accurint. Field examiners and coordinators inform the T31 NFBI system administrator of any necessary updates to SBU/PII information. The system administrator implements updates to ensure completeness, timeliness, and accuracy of the T31 NFBI database.

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 34.037 Audit Trail and Security Records

IRS 42.031 Anti-Money Laundering/Bank Secrecy Act and Form 8300

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: Criminal Investigation Management Information System (CIMIS)
Current PCLIA: Yes
Approval Date: 4/22/2019
SA&A: Yes
ATO/IATO Date: 5/23/2019

System Name: Criminal Investigation General Support System (CI-1)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 5/29/2020

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

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).

Name: FinCEN
Transmission Method: Manual
ISA/MOU: Yes

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

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: 50 States
Transmission Method: Manuel
ISA/MOU: Yes

Does the system receive SBU/PII from other sources?

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: Cipher Trace
Transmission Method: Manual
ISA/MOU: Yes

Organization Name: Chainanlysis
Transmission Method: Manual
ISA/MOU: Yes

Organization Name: Elliptic
Transmission Method: Manual
ISA/MOU: Yes

Organization Name: Internet
Transmission Method: Manual
ISA/MOU: No

Organization Name: Pipl
Transmission Method: Manual
ISA/MOU: Yes

Does the system receive SBU/PII from Taxpayer forms?

No

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: Criminal Investigation Management Information System (CIMIS)
Current PCLIA: Yes
Approval Date: 4/22/2019
SA&A: Yes
ATO/IATO Date: 5/23/2019

System Name: Criminal Investigation General Support System (CI-1)
Current PCLIA: Yes
Approval Date: 4/6/2020
SA&A: Yes
ATO/IATO Date: 5/29/2020

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 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.

Does this system disseminate SBU/PII to other Federal agencies?

Yes

Identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU).

Organization Name: FinCen
Transmission Method: Manual
ISA/MOU: Yes

Identify the authority.

31 CFR 1010.810 (b)(8). The Internal Revenue Service has been delegated authority to examine certain financial institutions, including money services businesses, to determine compliance with requirements of the Bank Secrecy Act.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

31 USC 5311 and 31 USC 5319.

For what purpose?

To share information with FinCen is a part of our delegated authority. A MOU with FinCEN dated 9/24/2010.

Does this system disseminate SBU/PII to State and local agencies?

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: States
Transmission Method: Manual
ISA/MOU: Yes

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.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

31 USC 5311 and 31 USC 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. The Memorandum of Understandings with the States is to share the number of Title 31 violations identified during a BSA examination, which is not an income tax examination.

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?

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.

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

No

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.

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.

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

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

Bank Secrecy Act (BSA) users apply for access to a user specific domain via BEARS process. During the BEARS approval process, the BSA functional BEARS 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.

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.

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.

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?

5/18/2021

Describe 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.

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)?

Treasury FISMA Inventory Management System (TFIMS).

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?

The Continuous Monitoring and the Security Assessment and Authorization processes ensure that the controls continue to work properly in safeguarding the PII. System Administrators performs ongoing system installation, configuration, operation, maintenance, and monitoring, including administration of security controls or security-related components of the system. Annual information system security assessments, including technical control testing and updated risk analyses, are conducted in compliance with Treasury and applicable guidance. System authorizations are conducted and maintained in accordance with IRS-defined policy and frequencies identified in the Federal Information Processing Standards and the National Institute of Standards and Technology and all assessments, results, and reports, stored in Treasury's FISMA Inventory Management System (TFIMS).

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: 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