

Date of Approval: February 5, 2016

PIA ID Number: **1582**

---

## 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

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.

Title 31 Non-Banking Financial Institution Database, Title 31, 856 , Final Approved

Next, enter the **date** of the most recent PIA. 8/3/2014

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

No Addition of PII  
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

Were there other system changes not listed above? No .

3. Check the current ELC (Enterprise Life Cycle) 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

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        No    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)
- No         Individual Taxpayer Identification Number (ITIN)
- No         Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)
- No         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).

Title 31 will continue to truncate the Social Security Number (SSN). 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 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 a Unauthorized Access (UNAX) violation upon entry into the system.

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

6c. 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

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
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.

6d. Are there other types of SBU/PII used in the system? Yes

If **yes**, describe the other types of SBU/PII that are applicable to this system. Name, TIN, Address, Telephone

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

<u>No</u>	PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
<u>No</u>	SSN for tax returns and return information is Internal Revenue Code Section 6109
<u>No</u>	SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
<u>Yes</u>	PII for personnel administration is 5 USC
<u>Yes</u>	PII about individuals for Bank Secrecy Act compliance 31 USC
<u>Yes</u>	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.

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? 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

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

---

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 42.031 Anti-Money Laundering/Bank Secrecy Act (BSA) and F

Treas/IRS 34.037 Audit Trail and Security Records System

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. N/A

---

**E. INCOMING PII INTERFACES**

---

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

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

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

<b><u>System Name</u></b>	<b><u>Current PIA?</u></b>	<b><u>PIA Approval Date</u></b>	<b><u>SA &amp; A?</u></b>	<b><u>Authorization Date</u></b>
Criminal Investigation (CI)	No		No	

11b. 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).

<b><u>Organization Name</u></b>	<b><u>Transmission method</u></b>	<b><u>ISA/MOU</u></b>
FinCEN	Manual	Yes

11c. Does the system receive SBU/PII from State or local agency (-ies)? 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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
50 States	Manual	Yes

11d. 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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
Internet	Manual	No

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

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

If **yes**, identify the forms  
No Employee Form Records found.

---

## 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? Yes

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

<u>System Name</u>	<u>Current PIA?</u>	<u>PIA Approval Date</u>	<u>SA &amp; A?</u>	<u>Authorization Date</u>
CI	No		No	
Other IRS Business Units	No		No	

Identify the authority and for what purpose? 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). All items are required for the business purpose of the system. The system is designed to identify, build, and monitor Title 31 examination cases.

12b . Does this system disseminate SBU/PII to other Federal agencies? Yes

If **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)

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
FinCEN	Manual	Yes
CI	Manual	Yes
States	Manual	Yes

Identify the authority and for what purpose? 31 USC 5311 and 31 USC 5319 Criminal Investigation (CI) – IRS Agency – Examination Case Selection (ECS) staff must obtain clearance information from CI to ensure the Money Service Business (MSB) is not being investigated for criminal activity by CI before they can assign a case to a field group. The Title 31 application contains a field entitled "CI Clearance". The "CI Clearance date" is updated when CI provides the clearance for Bank Secrecy Act (BSA) Examination to review the entity. ECS also receives "leads" via e-mail or "information requests" from CI on possible entities to review based on information received from Customs or US Immigration and Customs Enforcement (ICE). The system does not receive any information from a generated CI application. Financial Crime Enforcement Network (FinCEN): Treasury Agency – FinCEN is an agency under the purview of the Department of Treasury. Its mission is to enhance U.S. national security, deter and detect criminal activity, and safeguard financial systems from abuse by promoting transparency in the U.S. and international financial systems. IRS BSA provides a quarterly report to FinCEN on the number of examinations conducted within each state, number of financial institutions cited for violations and type of violation. This information is obtained from the information received from the Money Service Business (MSB) MOU Exchange Program. FinCEN sends an MSB agent list to the IRS ECS staff. ECS users will manually compare the entities listed on the agent list to the entities listed on the Title 31 application. Any entities listed on the agent list, but not on the Title 31 application will be manually updated to the Title 31 application.

12c. 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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
States	Manual	Yes

Identify the authority and 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 an 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 NBF1 examinations, and other State and NBF1 information - information that is collected in the course of screening, licensing, chartering and examining MSBs and NBFIs. The following state's tax Administration offices send data to Title 31 application users that are manually entered: Alabama Connecticut Indiana Alaska Delaware Kansas Arizona Florida Kentucky Arkansas Georgia Louisiana California Idaho Maine Colorado Illinois Maryland Massachusetts New Hampshire Oregon Minnesota New York Pennsylvania Mississippi North Carolina Puerto Rico Missouri North Dakota South Dakota Nebraska Ohio Tennessee Texas Washington Wyoming Utah West Virginia Vermont Wisconsin

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.

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

18b. If 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.

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

<b>IRS Employees?</b>	<b>Yes/No</b>	<b>Access Level(Read Only/Read Write/Administrator)</b>
-----------------------	---------------	---

Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	No	

Contractor Employees? No

21a. 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.

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 ?  
Not Applicable

---

## 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.

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 for Collection when next updated/published.

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? 3/17/2015

23.1 Describe in detail the system s audit trail. The Title 31 application has application files, data files , and application-specific logs that reside on a Wintel application server, This audit plan focuses on the Title 31 application specific requirements not fulfilled by the operating system; therefore, the reader will see several "Refer to Audit Plan" on the requirements tables. For details on how these audit plans fulfill

the requirements the reader can consult the Windows, Active Directory and MSSQL Audit Plans. Audit events that are application-specific are recorded in an audit trails log but could also be recorded in the trace logs, transaction logs or error logs. This application has a temporary audit log that is located on the Wintel Server. Since the application processes PII data all action taken on that data (read, create modify, delete, etc...) must be recorded to the application audit trails log. The PII information on entities is as follows: Name, TIN, Address, Telephone Number, State, and City. The PII information on Employees is as follows: Name and SEID. Determining what, when, and by whom specific actions were taken on a application system is crucial to establishing individual accountability, monitoring compliance with security policies, and investigating security violations. Audit events that are application-specific are recorded in and an audit trails log and are recorded in the Structured Query Language (SQL) Trace logs, transaction logs or error logs.

---

## 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?

The Continuous Monitoring and the Security Assessment and Authorization processes ensure that the controls continue to work properly in safeguarding the PII.

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

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: 100,000 to 1,000,000  
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? Yes

If **yes**, describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring. Access to the Title 31 application consists of a pre-configured Open Database Communication (ODBC) utility that connects the Title 31 application to the MS SQL database. This ODBC is a standard application program interface (API) which only connects to the Title-31 MS Access database and no other IRS applications. The application and ODBC as implemented by Title-31 interfaces does not support the usage of encryption for transmission confidentiality. The System is on IRS Infrastructure and is protected by the General Support Services (GSS). Online5081 is used to control access to the System. The System has the capability to identify, locate, and monitor Title 31 Inventory, consisting of Money Service Businesses (MSBs) for report writing purposes.

---

## **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**

---