Date of Approval: **August 21, 2023**

PIA ID Number: **7925**

SYSTEM DESCRIPTION

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

Bank Secrecy Act Exam Case Management (ECM) 8300 S, 8300 SharePoint Site

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?

Bank Secrecy Act Exam Case Management, SBSE BSA

What is the approval date of the most recent PCLIA?

8/25/2021

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Significant System Management Changes

New Access by IRS employees or Members of the Public

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.

935531000102010100 (55-31-31211) SB/SE Deputy Commissioner Examination Exam Deputy Operations Headquarters Examination Exam Case Selection Exam Case Selection-Specialty Bank Secrecy Act (BSA)

Current ELC (Enterprise Life Cycle) Milestones:

System Development/Milestone 4B

System Deployment/Milestone 5

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 Banking Secrecy Act (BSA) Exam Case Management 8300 SharePoint site collection will be used to build and manage case inventory. The 8300 SharePoint site will incorporate workflows that will allow Exam Case Selection (ECS) to build new cases and assign them to the various field groups. The field group managers will assign cases to specific examiners. The examiners will document the examination, backup their inventory, and close cases to their manager all within the SharePoint site. The group manager will review in-process and completed cases and will close cases to Currency Transaction Report (CTR) Operations. Cases that have been closed out will be stored on the SharePoint site for later retrieval, as needed. In addition, SAR (suspicious activity report) data is kept on this site. The SAR data is zipped, encrypted and password protected.

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:

Interfaces with external entities that require the SSN
Law enforcement and intelligence purposes

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

Bank Secrecy Act ECM 8300 SharePoint Site requires the use of SSN's because no other identifier can be used to uniquely identify a taxpayer. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. The 8300 SharePoint site Exam Case Selection (ECS) site Social Security Number (SSN) or Tax Identification Number (TIN) will be used to identify the taxpayer or subject of a Banking Secrecy Act (BSA) Non-Bank Financial Institution examination.

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

The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use Social Security Numbers (SSNs), which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. The SharePoint site collection 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.

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
Mailing Address
Phone Numbers
E-mail Address
Date of Birth
Place of Birth
Standard Employee Identifier (SEID)
Mother's Maiden Name
Protection Personal Identification Numbers (IP PIN)
Internet Protocol Address (IP Address)
Criminal History
Medical Information
Certificate or License Numbers
Vehicle Identifiers
Passport Number
Alien Number
Financial Account Numbers

Photographic Identifiers
Biometric Identifiers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

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.

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.

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.

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.

Employee Standard Employee Identifiers (SEIDs) will be used to identify employees who worked a particular case and will be used to make case assignments and monitor case inventory.

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)

SSN for tax returns and return information is Internal Revenue Code Section 6109

PII about individuals for Bank Secrecy Act compliance 31 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.

The SSN or TIN, along with Master File Tax Code (MFT) and Tax Period will be used to identify a unique case. The 8300 site within the BSA ECM site contains Suspicious Activity Report (SAR). This data will be zipped, and password protected to try to protect the data to the ultimate limit of our ability.

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

The 8300 coordinator creates the case in SharePoint by inputting the required case identifying information including form 9984, Case classification Sheet, Bank Currency Transaction Report (BCTR) Summary and BSAR information. Also includes Information Data Retrieval System (IDRS), Accurint, Examination Returns Control System (ERCS) data and the Workload Initiative Feedback Sheet. These case documents include SSN's, TIN's, Name, Address, City, State and Zip code data. Additional data may include Master File Tax (MFT) data and Tax Period data and additional taxpayer data such as a phone number. The case is assigned to the field group based on geographical location. The field group manager assigns the case to the examiner. The examiner gathers information from the individual being examined, third-parties, public data sources, and internal IRS sources and documents the case file. The completed case is reviewed by the group manager for accuracy, timeliness, and completeness. The completed case is reviewed by Cash Currency Transaction Report (CTR) Operations and updated to a closed status.

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 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: IDRS
Current PCLIA: Yes
Approval Date: 10/26/2021
SA&A: Yes
ATO/IATO Date: 3/6/2023

System Name: Financial Crimes Enforcement Network(FinCEN) BCTR/BSAR
Current PCLIA: No
SA&A: No

System Name: ACCURINT
Current PCLIA: No
SA&A: No

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: Financial Crimes Enforcement Network(FinCEN)
Transmission Method: Encrypted Disk couriered by Treasury Security
ISA/MOU: Yes

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

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

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

Yes

Please identify the form number and name:

Form Number: 8300
Form Name: Report of Cash Payments Over $10,000 Received in a Trade or Business

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?

At the onset of the transaction requiring the collection of the data used and provided on the 8300 BSA ECM SharePoint Site. The individual/or business received notification of the information being collected and reported to the IRS.

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

No

Why not?

Because suspicious pattern has been observed. For example, the method of Structuring. An individual or business will buy a car for 7,500 on one day and the next day, buy another car for 7501.00 on the following day. Then the next month the same type of activity will occur. If that happens, it could be deemed as suspicious, and a SAR will be filed on the business or individual via FinCEN.

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

The 8300 SharePoint is a closed system within the IRS/BSA ECM division. The site is only viewed by authorized personnel and not accessible to the public. CTRs and SARs are issued by/on entities subject to BSA laws when large or unusual transactions occur. A business subject to Form 8300 examinations is required to file a Form 8300 on certain transactions. For example, a person walking into a car dealership with 15,000 dollars cash and buying a car requires the car dealership to file a Form 8300 on the transaction. The individual is notified that a Form 8300 has been filed and that information has been transmitted to the IRS.

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

Developers: Administrator

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

The Banking Secrecy Act Exam Case Selection (BSAECM) SharePoint site 8300 site collection is owned by a Senior Program Analyst (analyst) under the authority of the Program Manager of Examination Case Selection. Upon approval by the Program Manager, the analyst will act as the Site Content Owner (SCO). The access is limited to Exam Case Selection (ECS), Banking Secrecy Act (BSA) Site Owner. Users will request access through the SharePoint interface and an email will be sent to the designated party on the SharePoint Site Collection. Site Collection Owners (SCO), who are generally HQ Analysts or Managers, will be responsible for determining who has access to their individual site collections. An email is currently forwarded to the Business Unit Representative (BUR) for this site collection for any access requests. The BUR will contact the SCOs to determine if the access is appropriate prior to granting. Individuals that are denied access will be given specific information as to why and, if warranted, what is needed to have access via an email from the BUR. SCO tracks who needs to have access to the site and their respective rights to the content. The Small Business/Self Employed (SB/SE) Administration Team (SPAT) will be the site collection administrators. Groups with specific permissions will be created to address the controlled access requirements of the site collection and its linked sites, document libraries and lists. In cases where there are access requests, the Out of the Box (OOB) access request list will receive the request and document who made and approved the request. This information is kept on an administration page on the site. In limited situations where the BUR or SCO does not know the requester, the requestor's manager will need to confirm that the requestor has a need to know, and access is required. Emails will be retained to document the authorization.

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.

The records are required to be maintained for 3 years. After 3 years on case files have passed, the records are sent to electronic archive. After a period of 7 years, the records are marked for deletion should the program manager request it. Since these records are maintained in electronic format, they can be kept stored indefinitely. RCS 23 Item 42- Examination Case Files. Copies of Revenue Agent reports with related work papers and other documents filed in the Examination organizations. Examination Case Files. Copies of Revenue Agent reports with related work papers and other documents filed in the Examination organizations. a) Fraud Cases. (Job No. N1-58-88-4) AUTHORIZED DISPOSITION Retire to Records Center 3 years after the date of closing. Destroy 10 years from the date of closing. b) Coordinated Industry Cases. (Job No. N1-58-88-4) AUTHORIZED DISPOSITION Retire to Records Center 4 years after the date of closing. Destroy 15 years from the date of closing. c) Case File Closing Agreements. PENDING DISPOSITION Instructions/final retention are under IRS stakeholder review. Contact Exam IRC regarding status.

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?

Yes

Describe the system's audit trail.

"Case Folder Actions" which tracks when a user updates a case via the Access interface. This does create an audit trail for these events but does not track when a user logs in and out of the system. When a user logs in and out of the system is tracked at the SharePoint User Group Level (SPAT). The system will track documents and case folders when they are opened or changed. If an audit log is needed to be viewed, our group can request the audit log for that user.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

This system doesn't have a system security plan, this system is composed of SharePoint sites and privacy testing for SharePoint is documented within Microsoft 365. In addition, PII is received from IDRS, and privacy testing is completed for IDRS.

SBU DATA USE

Does this system use, or plan to use SBU Data in Testing?

Yes

Was permission granted per the requirements of Form 14664, SBU Data Use Questionnaire or Form 14665, SBU Data Use Request?

Yes

Provide the date the permission was granted.

7/7/2021

Was testing performed in conformance with IRM 10.8.8 Information Technology (IT) Security, Sensitive But Unclassified (SBU) Data Policy?

Yes

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?

No