Date of Approval: **October 27, 2023**

PIA ID Number: **7816**

SYSTEM DESCRIPTION

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

Joint Automated Booking System, JABS

Is this a new system?

Yes

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

Criminal Investigations Governance Board (CIGB)

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

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.

Internal Revenue Service - Criminal Investigation (CI) is the law enforcement arm of the Internal Revenue Service. CI is charged with the enforcement of the federal income tax statutes. CI's top priority is the investigation of violations of the federal income tax law. Additionally, CI special agents lend their financial investigative expertise to money laundering and narcotics investigations conducted in conjunction with other law enforcement agencies at the local, state and federal levels. The Fix NICS Act was recently passed into law requiring all agencies, including IRS, to submit Forms R84 and fingerprint cards to the FBI's Criminal Justice Information System (CJIS) related to the following categories: 1) Persons under indictment; 2) Fugitives from justice; and 3) Persons with felony or misdemeanor convictions. The United States Marshal Service (USMS) was used to book and process arrestees, which consisted of electronic fingerprint scanning, photographs, and biographical data that was submitted directly to the FBI CJIS through the Joint Automated Booking System (JABS). IRS special agents would then obtain a copy of the electronic fingerprint

card that would be either mailed or faxed to the FBI CJIS along with the Form R-84. In the Cincinnati Field Office, for example, the USMS would no longer process arrestees for the IRS, particularly self-reporting individuals. In compliance with the Fix NICS Act of 2017, IRS-CI will process its own arrestees, as also promulgated in IRM 9.4.12.13 (12-13-2010) Processing the Arrested Person.

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

Legal/statutory basis (e.g. where collection is expressly required by statute)

Statistical and other research purposes

Delivery of governmental benefits, privileges, and services

Law enforcement and intelligence purposes

Another compelling reason for collecting the SSN

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

The system application is for arresting and booking an individual and require all PII information to put them 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).

The system will use the CJIS required encryption to mask data. Forecasted implementation date is December 2023.

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
Phone Numbers
Date of Birth
Criminal History
Alien Number
Photographic Identifiers
Employment Information
Mailing 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.

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?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Date of birth, Gender, Height, Weight, Hair color, Employer, Employer address, Eye-color, Citizenship, Address, SSN, Miscellaneous numbers, FBI number, Armed forces Number, Aliases

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

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.

The system application is for arresting and booking an individual and require all PII information to put them into the system. They are: Name, mailing address, phone numbers, date of birth, Gender, Height, Weight, Hair color, Employer, Employer address, Eye-color, Citizenship, Address, SSN. We are arresting this individual and need all this data to support the business need: to properly identify the individual. It clearly supports the CI mission which is enforcement of the Tax Code.

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

The Criminal Investigation Agents from the individual's history know who and why they are arresting due to their tax aggression. Thus, they would have to arrest that person from their tax history.

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 46.002 Criminal Investigation Management Information System and Case Files

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?

No

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?

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 individual is being arrested, has basically no rights and notice is not appropriate.

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

No

Why not?

Because they are being arrested.

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

The individuals are read their Miranda rights during their arrest.

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 Only
System Administrators: Administrator
Developers: Administrator

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

User accounts and permissions have been identified by the System Owner and the Senior Analyst. A separate computer will be used for this purpose and agents will log in with their SmartID.

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.

These arrest records entered into the Joint Automated Booking System (JABS) identified in the PCLIA are scheduled as permanent by the system owner (DOJ/FBI). DOJ NARA Job number N1-060-00-011.

SA&A OR ASCA

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

In-process

When is the anticipated date of the SA&A or ACS completion?

11/30/2023

Describe the system's audit trail.

The Audit Trail Report can be displayed through a built in Preview window. It can be printed directly to any printer that is configured for that computer. It can also be exported in the following formats: PDF, HTML, MHT, RTF, DOCX, XLS, XLSX, CSV, TXT, and Image File (BMP, EMF, WMF, GIF, JPEG, PNG, TIFF). You must have permission to View the Audit Trail in order to print reports. The Audit Trail Search is another way to generate a report. It can be printed directly to any printer that is configured for that computer. It can also be exported in the following formats: PDF, DOCX, XLS, XLSX, HTML, RTF, and TXT. You must have permission to View the Audit Trail in order to print reports.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

No

When is the test plan scheduled for completion?

9/1/2023

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?

Currently identifying security requirements. Building out environments.

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: Under 100,000
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