Date of Approval: **May 19, 2021**

PIA ID Number: **5845**

SYSTEM DESCRIPTION

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

Safeguards Database, Safeguards DB

Is this a new system?

Yes

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

None

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

Domain Architecture/Milestone 2

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

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 Office of Safeguards is located within the Government Liaison, Disclosure, and Safeguards (GLDS), which is within the Privacy, Governmental, Liaison Disclosure (PGLD). The Office of Safeguards ensures federal tax information (FTI) provided outside the IRS is protected in accordance with IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies. The Office of Safeguards has oversight of federal, state and local agencies / entities that receive federal tax information; conducts onsite reviews to identify physical and computer security control weaknesses; monitors compliance through Corrective Action Plans (CAP), ensures Internal Revenue Code § 6103 disclosure restrictions are adhered to by agencies and manages external data incidents. The data gathered from the onsite reviews are stored in an external application called eCase. The data elements such as Issue Code, Status, Issue Date, Days Overdue, Case Type, Case Number, Extension date, Report date, Latest Review date, CAP due date, Safeguard Review Report (SRR) received

date, Safeguard Security Report (SSR) received date, will be ingested into the new database and modeled for internal Office of Safeguards reporting and analytical purposes. Currently, the Office of Safeguards generates quarterly reports for its internal risk analysis process. These reports are currently not stored in a database where they can be modeled for additional reporting and analytics purposes. Additionally, the current process adds hours of manual labor due to the inability to automate the data lifecycle. Implementing the Safeguards-DB Project will eliminate the need to manually download data files and compile reports.

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.)?

No

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

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:

Physical Security Information Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities.

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

No

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

PII for personnel administration is 5 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 does not store SSNs but names of the personnel of the state and local government agencies who have entered the security vulnerability. The Office of Safeguards conducts reviews at these agencies to ensure that they are following guidelines of Publication 1075 and IRC 6103.

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

The accuracy, timeliness, completeness of the information within the source system (eCase) is done at the time it is entered.

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 36.003 General Personnel and Payroll Records

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: TRACMS
Current PCLIA: Yes
Approval Date: 8/20/2018
SA&A: No

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

No

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)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

No

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

No

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

No

Does this system disseminate SBU/PII to IRS or Treasury contractors?

Yes

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

Organization Name: Booz Allen Hamilton
Transmission Method: Email
ISA/MOU: No

Identify the authority.

Internal Revenue Code (IRC) Section 6103(p)(4) gives responsibility to ensure that all safeguard requirements are met when federal, state, and local agencies obtain return information.

For what purpose?

Yes

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?

Yes

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.

This is an internal database that will be used for our reporting and the data does not contain personal individual data.

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

No

Why not?

Not applicable

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

The data is a dump or copy of the source data. It will have been validated upon entry into that system.

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: Administrator

System Administrators: Administrator

Developers: Administrator

IRS Contractor Employees

Contractor Users: Read Only

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

The users will be added using the SQL Server Management Console. They will need manager approval.

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.

RCS 8 Item 101-Safeguard Reports. Files consisting of procedures, reports, and work papers pertaining to the planning and executing of safeguard reviews pursuant to IRC Section 6103. (Job No. N1-58-00-1) A. Safeguard Procedures Reports. The federal or state agency's description of how federal tax information will be processed and protected from unauthorized disclosure. AUTHORIZED DISPOSITION Cut off files annually. Destroy after 2 subsequent Safeguard Procedures Reports are received. B. Safeguard Activity Reports. The

federal or state agency's annual report advising IRS of minor changes to the procedures or safeguards specified in the Safeguard Procedures Report, actions on review recommendations, current annual activities, and planned actions affecting procedures. AUTHORIZED DISPOSITION Cut off files annually. Destroy when 5 years old. Safeguard Review Reports and Work papers. Reports of IRS on-site evaluations of federal, state, or local agencies' practices for safeguarding federal tax returns and/or return information. AUTHORIZED DISPOSITION Cut off files annually. Destroy after 2 subsequent reviews are completed. D. Reference/Management Reports. AUTHORIZED DISPOSITION Cut off files annually Destroy when 3 years old.

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.

The Enterprise Operations (EOps) team will administer, manage the Windows 2012 VM server as well as the SQL Server 2019 database on it. EOps will conduct backups, but at this time, the server has not been completed and have not received audit or security information.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

This is a database install project with no interface.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: Not Applicable

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