Date of Approval: **April 06, 2020**

PIA ID Number: **4883**

SYSTEM DESCRIPTION

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

Criminal Investigations General Support System, CI, CI-1 GSS

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?

Criminal Investigations General Support System, CI-1, # 2054

What is the approval date of the most recent PCLIA?

4/26/2017

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.

Criminal Investigation Governance Board (CIGB)- Reports to Sustaining Ops (SO) Executive Steering Committee (ESC). Governs projects in the portfolios for those business and functional divisions not wishing to create their own separate boards; ensures adherence to Enterprise Life Cycle; manages scope, cost and schedule variances; escalates issues to Enterprise Governance (MEG) Committee or the appropriate 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.

Criminal Investigation (CI) serves the American public by investigating potential criminal violations of the Internal Revenue Code and related financial crimes in a manner that fosters confidence in the tax system and compliance with the law. The CI-1 GSS is integral in supporting the mission of CI as the GSS provides network connectivity to internal CI applications. The CI network provides users with the necessary infrastructure to access e-mail services, file services, print services, and access to management and inventory database systems. The network operates on top of the IRS wide area network (WAN) with CI local area network (LAN) segments isolated behind CI routers for additional layer of security. Due process is provided outside of the system pursuant to 26 USC and 18 USC.

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:

Statistical and other research purposes

Law enforcement and intelligence purposes

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

User SSNs serve as an essential data bit for use in identifying a user's record.

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 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. Criminal Investigations General Support System requires the use of SSN's 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 return.

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

E-mail Address

Date of Birth

Standard Employee Identifier (SEID)

Internet Protocol Address (IP Address)

Criminal History

Certificate or License Numbers

Vehicle Identifiers

Passport Number

Alien Number

Financial Account Numbers

Photographic Identifiers

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

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)

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

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.

Anything potentially related to Criminal Investigations. This may include extracts from other sources such as Criminal Investigative Division (CID) Inventory (INV) Individual Master File (IMF) and Document Manager (DocMgr). Criminal Investigation Desktop Application (DocMgr) is a desktop application like MS Word, Excel, and PowerPoint. The Criminal Investigation Division IMF Inventory (CID IMF INV) extract is used as a data source for PII information.

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

The CI-1 Information System Security Officer (ISSO) is responsible for the updating of this information with major application owners being responsible for the integrity of the provided data.

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

IRS 46.050 Automated Information Analysis System

IRS 34.037 Audit Trail and Security Records

IRS 46.005 Electronic Surveillance and Monitoring 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?

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?

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?

The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number.

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

No

Why not?

The information is collected while carrying out the Internal Revenue laws of the United States; an individual cannot decline providing the information.

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

Publication 1 "Your Rights as a Taxpayer" explains the rights of the taxpayer, which includes the right to challenge the IRS' position and be heard; and the right to appeal an IRS decision in an independent forum. Individuals under investigation do not lose their right to due process, as dictated by the Internal Revenue Manual guidelines. IRS policy allows individual taxpayers whose data is in the system the opportunity to clarify or dispute negative determinations through the appeals process. However, due to the nature of this system, individuals may not receive specific notice that their information has been collected.

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?

Data and system owners make decisions regarding access, these decisions are approved and documented in the employees' Online OL5081.

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.

CI-1 General Support System (GSS) is non-recordkeeping. It provides infrastructure support and data security to servers that host CI-related applications. Disposition instructions for CI recordkeeping systems are published under IRM 1.15.30 (soon to transition to Records Control Schedule (RCS) Document 12990, under RCS 30) for Criminal Investigation Records, and/or RCS 20 for Administrative/Organization Support Operational Records (already published in Document 12990). GRS 3.1 Item 010-Infrastructure project records-Destroy 5 years after project is terminated, but longer retention is authorized if required for business use.

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?

5/29/2020

Describe the system's audit trail.

The following data types are collected in the audit trail: -Date/Time Stamp (The Date/Time of when the audit record was created) -Unique Identifier (The Unique Identifier that initiates the action for the audit record, such as the user name or SID) -Event Type (The Event Type field is used to track the type of event that is executed such as create, update, or delete) -Origin of Request (The origin of where the request was made, such as the Terminal ID) -Name of Object (The name of the object that was introduced, accessed, or deleted) -User Identity (The identity of the user who performed the action) -User Role (The role of the user at the time the action was performed).

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

The CI-1 GSS consist of Commercial Off the Shelf (COTS)products that are engineered together into an infrastructure/architecture that provide some level of service or support to the applications that reside on them. Developer activities, to include configuration, developer security testing and evaluation, development process, standards, tools, developer-provided training, and developer security architecture and design are handled by the individual application. Any responsibilities for implementing control requirements for these activities are the responsibilities of the applications and not applicable to the underlying infrastructure support.

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: Under 5,000

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