Date of Approval: **June 25, 2019**

PIA ID Number: **4121**

SYSTEM DESCRIPTION

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

International Business Machines Platform GSS-21, IBM GSS-21

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?

International Business Machines Platform. # 3615

What is the approval date of the most recent PCLIA?

8/31/2018

Changes that occurred to require this update:

Significant Merging with Another System

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.

EOps Security Operations and Standards (SOSD) Director, is responsible for security governance of this GSS.

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.

GSS-21 is an Internal Revenue Service (IRS), Enterprise Operations Services (EOps) infrastructure support information system that has been categorized as a General Support System (GSS). GSS-21 is comprised of four mainframe computers housed in separate locations. The system is divided into multiple Logical Partitions (LPARs) that host and provide infrastructure support for the systems that reside on them. Those systems (4) include:
* Masterfile System
* Integrated Collection System (ICS), Automated Collection System (ACS), and the Printer Replacement to Integrate New Tools (PRINT), major applications. Together, these three major applications - ICS, ACS and PRINT - are referred to as the IAP platform.
*Security and Communication System (SACS)
*Computer Assisted Publishing System (CAPS)
The Masterfile applications that reside on GSS-21 process taxpayer data which resides in the databases on the mainframe. The IAP System serves as an intermediary for Unisys, Security and Communications System (SACS), and the Master File systems, and also acts as the liaison between the Service and National Print Centers. The IAP major applications generate the content for all IRS Notices to taxpayers. The SACS System is the communications front end processor and message processing system utilized by IRS employees who access the Integrated Data Retrieval System (IDRS), Corporate Files Online (CFOL) and Electronic Federal Payment Posting System (EFPPS) applications. SACS provides user and application security validation for access to these applications including, identification and authentication (I&A), access controls, and audit logging functions. The IDRS, CFOL and EFPPS applications are directly supported by the GSS-21 and GSS-23 GSSs and IRS users access these applications via SACS. It also consists of key aspects of the Computer Assisted Publishing System (CAPS) and provides infrastructure support for that project. The CAPS application provides computer resources required by the IRS Media & Publications (M&P) organization to develop, design, produce, procure and, and distributes the full range of tax forms, instructions, publications, etc. for both internal and public use. CAPS utilizes the Internal Revenue Service (IRS) Transmission Protocol/Internet Protocol (TCP/IP) backbone for all network functions.

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)

When there is no reasonable alternative means for meeting business requirements

Statistical and other research purposes

Delivery of governmental benefits, privileges, and services

Law enforcement and intelligence purposes

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

SSN's, being unique taxpayer ID numbers, are collected and used by the system in order to administer the tax code of the United States as mandated by Congress. This includes the collection of taxes and compiling statistical data on the payment of taxes. Other agencies access this data in order to enforce laws pertaining to various forms of money laundering.

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, Managing Information as a Strategic Resource 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. GSS-21 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 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)

Protection Personal Identification Numbers (IP PIN)

Financial Account Numbers

Employment Information

Tax Account Information

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 (SBUList)

Agency Sensitive Information - Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission

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.

Federal Tax Information

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

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

PII for personnel administration is 5 USC

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.

This GSS hosts and provides primarily support for application programs and databases for the Employees Plans Masterfile (EPMF), the Information Returns Masterfile (IRMF), the Individual Masterfile (IMF), the Business Masterfile (BMF), and the Payer Masterfile (PMF) Masterfile applications along with Currency & Banking Retrieval System (CBRS), Tax Litigation Counsel Automated Tracking System (TLCATS), Integrated Data Retrieval System (IDRS), Automated Collection System (ACS), Integrated Collection System (ICS) and other user facing systems. Each of the applications listed above have daily, weekly, and quarterly runs and contain taxpayer data. The IAP system provides infrastructure support for the Integrated Collection System (ICS), Automated Collection System (ACS), and report distribution software (Print). Together, these three major applications are referred to as ICS, ACS, and PRINT (IAP). The National Print Center located at ECC-Detroit uses IAP major applications to generate the content for all IRS notices to taxpayers. This infrastructure supports major aspects of the Wage and Investment Computer Assisted Publishing System (W&I CAPS) application and application Commercial Off the Shelf (COTS), which in turn supports the design, composition, requisitioning, printing procurement and job tracking for the entire complement of IRS published products. Because of the nature of the various applications that run on GSS-21, there is a need for the GSS to store and maintain the various forms of SBU/PII that reside on the GSS. This data is used by many of the applications to administer the tax code of the United States as it relates to the collection of taxes and enforcement of the applicable tax code, whether that code relates to individual or businesses. For instance, IMF stores individual taxpayer data which requires the use of the individual's SSN to identify the individual, while BMF uses the businesses EIN to identify the business. For the SACS component the SSN's are used on the SACS system to enforce negative TIN checking to administer IDRS in accordance with the National Institute of Standards & Technology (NIST) and Internal Revenue Manual (IRM) regulations. This data is also used to produce statistical tax data that is used by different government organizations to provide reports to Congress and other organizations.

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

GSS-21 provides infrastructure support for the Masterfile and IAP major applications. It is the applications that reside on the GSS that are responsible for verifying the accuracy, timeliness, and completeness of data that is processed, stored and transmitted from the GSS.

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.

Treasury/IRS 34.037 Audit Trail and Security Records System

Treasury/IRS 24.030 Customer Account Data Engine Individual Master File

Treasury/IRS 24.046 Customer Account Data Engine Business Master File

Treasury 009 Treasury Financial Management Systems

RESPONSIBLE PARTIES

Identify the individuals for the following system roles:

For 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?

Yes

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

No

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

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).

Organization Name: Social Security Administration

Transmission Method: Electronic Database

ISA/MOU Yes

Organization Name: Bureau of Fiscal Serivce (BFS)

Transmission Method: Electronic Database

ISA/MOU Yes

Organization Name: Health and Human Services

Transmission Method: Electronic Database

ISA/MOU No

Organization Name: Department of Education

Transmission Method: Electronic Database

ISA/MOU Yes

Organization Name: Census Bureau

Transmission Method: Electronic Database

ISA/MOU No

Identify the authority

Authority to disseminate SBU/PII to other agencies is granted by the Congress which gives the IRS the authority to administer any and all applicable tax laws.

Identify the Routine Use in the applicable SORN (or Privacy Act exception)

Routine use is in the administration of the US tax code.

For what purpose?

To collect the proper amount of tax from all taxpayers, whether businesses or individuals.

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

No

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

No

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?

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?

Providing this information is a requirement for filing taxes. For the SACS component the negative TIN file is used by the SACS system to ensure that IDRS personnel only examine appropriate cases.

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

Not Applicable --- As a general support system, GSS-21 only provides infrastructure support for the Masterfile and IAP major applications. GSS-21 does not make determinations. All determinations are completed through the collection process by the applications with no direct correlation to GSS-21.

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: Read Write

IRS Contractor Employees

Contractor Users: Administrator

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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

File/IAP/CAPS Platform is requested via an Online Form (OL) 5081. Access is granted on a need-to-know basis. The OL5081 enrollment process requires that an authorized manager approve access requests on a case by case basis. Access approval is based on the Users role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments, they are restricted from changing the boundaries of their access without management approval. The employee's access will be terminated once they no longer require access to the Database. Deletion from the active access role is also performed through the OL5081. This control is enforced by Resource Access Control Facility (RACF) Security settings on the user's account.

RECORDS SCHEDULE

Are these records covered under a General Records Schedule (GRS, IRS Document 12829), or has the National Archives and Records Administration (NARA) archivist 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 Information Technology (IT) General Support System (GSS-21) is non-recordkeeping. GSS-21 provides network infrastructure and platform support for the Masterfile, Integrated Collection System (ICS), Automated Collection System (ACS), and the Printer Replacement to Integrate New Tools (PRINT) major applications. Each recordkeeping application residing on GSS-21 has its own retention period. Audit logs are maintained in accordance with General Records Schedule (GRS) 3.2, Item 031. For IRS systems that store or process taxpayer information, audit trail archival logs are retained for 7 years, unless otherwise specified by a formal Records Control Schedule developed in accordance with IRM 1.15, Records Management. At the end of the standard maintenance period, the audit logs are reviewed to determine if the logs require additional retention at the Federal Records Center or if destruction is appropriate. Additional guidance is provided in IRM 1.15. Database audit data is not required to be local to the database for the period of retention but is available for historical analysis if needed. Audit data is only readable by personnel authorized by the security specialists (SecSpec).

SA&A OR ASCA

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

Yes

What date was it completed?

2/8/2019

Describe the system's audit trail.

The MITS-21 GSS audit trail includes an employee's UserID, time of login and logoff, the event that occurred and the associated date and time. In addition, the audit trail captures the success or failure of each action, the terminal from which the action was initiated, and the component accessed.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

If yes, where are test results stored (or documentation that validation has occurred confirming that requirements have been met)? Test results are stored on the Treasury FISMA Inventory Management System (TFIMS) website.

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

Yes

Please describe the outstanding issues:

This system has open Plan of Action and Milestones (POA&M's) as a result of the Annual Security Control Assessment (ASCA) testing that takes places. These various weaknesses are being addressed and closed once the findings are mitigated by the appropriate staff members. A listing of the open POA&M's on the system can be seen on the TFIMS website.

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?

Annual Security Controls Assessment (ASCA) is performed annually to determine if selected System Security Plan (SSP) controls are operating as intended. This process ensures that all application information and control descriptions are updated and tested to ensure that the controls continue to work properly in safeguarding the PII. Findings from the ASCA are detailed in the Security Assessment Report (SAR) leading to the mitigation of the findings.

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: More than 1,000,000

Other: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

SEID, 10,000

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?

Yes

Does the system have a process in place to account for such disclosures in compliance with IRC §6103(p) (3) (A) or Subsection (c) of the Privacy Act? Contact Disclosure to determine if an accounting is required.

Yes