
A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. IBM Master File/IAP/CAPS Platform, GSS-21

2. Is this a new system? No

2.a. If **no**, is there a Privacy Civil Liberties Impact Assessment (PCLIA) for this system? Yes

If **yes**, enter the full name, acronym, and milestone of the most recent PCLIA.

Masterfile - IAP, GSS-21, Final Approval

Enter the approval **date** of the most recent PCLIA. 09/15/2016

If **yes** Indicate which of the following changes occurred to require this update (check all that apply).

- No Addition of Personally Identifiable Information (PII)(PII is any information that is linked or linkable).
- No Conversions
- No Anonymous to Non-Anonymous
- No Significant System Management Changes
- Yes Significant Merging with Another System
- No New Access by IRS employees or Members of the Public
- No Addition of Commercial Data / Sources
- No New Interagency Use
- No Internal Flow or Collection
- No Expiring PCLIA

If **yes**, explain what changes were made.

3. 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.

3.a. Check the current Enterprise Life Cycle (ELC) Milestones (select all that apply).

- No Vision & Strategy/Milestone 0
- No Project Initiation/Milestone 1
- No Domain Architecture/Milestone 2
- No Preliminary Design/Milestone 3
- No Detailed Design/Milestone 4A
- No System Development/Milestone 4B
- No System Deployment/Milestone 5
- Yes Operations & Maintenance (i.e., system is currently operational)

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

A.1 General Business Purpose

5. 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 three mainframe computers housed in separate locations. The system is divided into multiple Logical Partitions (LPARs) that host and provide infrastructure support for the Masterfile system and 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. It also consists of key aspects of the Computer Assisted Publishing System (CAPS) and provides infrastructure support for that project. The Masterfile applications that reside on GSS-21 process taxpayer data which resides in the databases on the mainframe. IAP 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 CAPS application provides computer resources required by the IRS Media & Publications (M&P) organization to develop, design, produce, procure and, and distribute 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.

B. PII DETAIL

6. Does the system use, collect, receive, display, store, maintain, or disseminate IR Code 6103 taxpayer information; or any type of Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII)?
Yes

6.a. If **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

If **yes**, check all types of tax identification numbers (TIN) that apply to this system:

<u>Yes</u>	Social Security Number (SSN)
<u>Yes</u>	Employer Identification Number (EIN)
No	Other Taxpayer Identification Number

If SSNs apply, which of the following approved Treasury uses of the SSNs applies:

<u>No</u>	Security background investigations
<u>Yes</u>	Interfaces with external entities that require the SSN
<u>Yes</u>	Legal/statutory basis (e.g. where collection is expressly required by statute)
<u>Yes</u>	When there is no reasonable alternative means for meeting business requirements
<u>Yes</u>	Statistical and other research purposes
<u>Yes</u>	Delivery of governmental benefits, privileges, and services
<u>Yes</u>	Law enforcement and intelligence purposes
<u>No</u>	Another compelling reason for collecting the SSN

Explain why one or more of the eight authorized uses above support the new or continued use of SSNs.

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 memorandum M-17-12 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. The IBM Master File/IAP/CAPS Platform 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.

6.b. Does this system use, collect, receive, display, store, maintain, or disseminate other (non-SSN) PII (i.e. Names, addresses, etc.)? Yes

If **yes**, specify the information.

<u>Selected</u>	<u>PII Element</u>
Yes	Name
Yes	Mailing address
Yes	Phone Numbers
Yes	E-mail Address
Yes	Date of Birth
Yes	Place of Birth
Yes	Standard Employee Identifier (SEID)
No	Mother's Maiden Name
Yes	Protection Personal Identification Numbers (IP PIN)
No	Internet Protocol Address (IP Address)
No	Criminal History
No	Medical Information
No	Certificate or License Numbers
No	Vehicle Identifiers
No	Passport Number
No	Alien Number
Yes	Financial Account Numbers
No	Photographic Identifiers
No	Biometric Identifiers
Yes	Employment Information
Yes	Tax Account Information
No	Centralized Authorization File (CAF)

6.c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? Yes

If **yes**, select the types of SBU

<u>Selected</u>	<u>SBU Name</u>	<u>SBU Description</u>
Yes	Agency Sensitive Information	Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission
No	Procurement sensitive data	Contract proposals, bids, etc.
No	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.
Yes	Proprietary data	Business information that does not belong to the IRS
Yes	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
No	Physical Security Information	Security information containing details of serious weaknesses and vulnerabilities associated with specific systems and facilities
No	Criminal Investigation Information	Information concerning IRS criminal investigations or the agents conducting the investigations.

6.d. Are there other types of SBU/PII used in the system? No

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

- Yes PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, 6012e(a)
- Yes SSN for tax returns and return information is Internal Revenue Code Section 6109
- No SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397
- Yes PII for personnel administration is 5 USC
- Yes PII about individuals for Bank Secrecy Act compliance 31 USC
- Yes Information by CI for certain money laundering cases may be 18 USC

6.f. Has the authority been verified with the system owner? Yes

B.1 BUSINESS NEEDS AND ACCURACY

7. 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. 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.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness?

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.

C. 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.

9. 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

If **yes**, enter the SORN number(s) and the complete the name of the SORN(s).

<u>SORNS Number</u>	<u>SORNS Name</u>
IRS 34.037	Audit Trail and Security Records System
IRS 24.030	Customer Account Data Engine Individual Master File
IRS 24.046	Customer Account Data Engine Business Master File
Treasury .009	Treasury Financial Management Systems

*IRS is required to have a published Privacy Act system of records in the Federal Register. Please identify the Privacy Act SORN(s) that cover these records. If you need additional assistance identifying the correct SORNS please email *Privacy.*

D. RESPONSIBLE PARTIES

10. Identify the individuals for the following system roles. ## Official Use Only

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? No

F. DISSEMINATION OF PII

12. Does this system disseminate SBU/PII? Yes

12.a. Does this system disseminate SBU/PII to other IRS Systems? No

12.b. Does this system disseminate SBU/PII to other Federal agencies? Yes
If **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).

<u>Organization Name</u>	<u>Transmission method</u>	<u>ISA/MOU</u>
Department of Education	Electronic Database	Yes
Census Bureau	Electronic Database	No
Health and Human Services	Electronic Database	No
Social Security Administration	Electronic Database	Yes
Bureau of Fiscal Service (BFS)	Electronic Database	Yes

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.

12.c. Does this system disseminate SBU/PII to State and local agencies? No

12.d. Does this system disseminate SBU/PII to IRS or Treasury contractors? No

12.e. Does this system disseminate SBU/PII to other Sources? No

G. PRIVACY SENSITIVE TECHNOLOGY

13. Does this system use social media channels? No

14. Does this system use privacy-sensitive technologies such as mobile, global position system (GPS), biometrics, Radio Frequency Identification (RFID), etc.? No
15. Does the system use cloud computing? No
16. Does this system/application interact with the public? No

H. INDIVIDUAL NOTICE AND CONSENT

17. Was (or is) notice provided to the individual prior to collection of information? Yes

17.a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide 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

18. Do individuals have the opportunity to decline from providing information and/or from consenting to particular uses of the information? No

18.b. If individuals do not have the opportunity to give consent, why not?
Providing this information is a requirement for filing taxes.

19. 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.

I. INFORMATION PROTECTION

20. 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

21. The following people have access to the system with the specified rights:

IRS Employees? Yes

<u>IRS Employees?</u>	Yes/No	Access Level (Read Only/Read Write/Administrator)
Users	Yes	Read and Write
Managers	Yes	Read and Write
Sys. Administrators	Yes	Administrator
Developers	Yes	Read and Write

Contractor Employees? Yes

<u>Contractor Employees?</u>	Yes/No	Access Level	Background Invest. Level
Contractor Users	Yes	Administrator	High
Contractor Managers	No		
Contractor Sys. Admin.	Yes	Administrator	Moderate
Contractor Developers	Yes	Read and Write	Moderate

21.a. How is access to SBU/PII determined and by whom? Access to the IBM Master 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.

I.1 RECORDS RETENTION SCHEDULE

22. Are these records covered under the General Records Schedule (GRS), or have a National Archives and Records Administration (NARA) archivist approved a Record Control Schedule (RCS) for the retention and destruction of official agency records stored in this system? Yes

22.a. If **yes**, how long are the records required to be held under the corresponding RCS and how are they disposed of? In your response, please include the complete IRM number 1.15.XX and specific item number and 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).

I.2 SA&A OR ASCA

23. Has the system been through Security Assessment and Authorization (SA&A) or Annual Security Control Assessment (ASCA)? In-process

23.b. If **in process**, when is the anticipated date of the SA&A or ASCA completion? 12/06/2018

23.1. Describe in detail 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24.a. If **yes**, If yes, was the test plan completed? Yes

24.a.1. 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.

24.a.2. If **yes**, were all the Privacy Requirements successfully tested? Yes

24.a.3. If **yes**, are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved? Yes

24.a.3.a. If **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.

24.1. Describe what testing and validation activities which have been conducted or are in process 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.

K. SBU Data Use

25. Does this system use, or plan to use SBU Data in Testing? No

L. NUMBER AND CATEGORY OF PII RECORDS

26. Identify the number of individual records in the system for each category:

- 26.a. IRS Employees: Under 50,000
26.b. Contractors: Under 5,000
26.c. Members of the Public: More than 1,000,000
26.d. Other: Yes

If **other**, identify the category of records and the number of corresponding records (to the nearest 10,000).

SEID, 10,000

M. CIVIL LIBERTIES

27. Does the system maintain any information describing how any individual exercises their rights guaranteed by the First Amendment? No

28. Is the system information used to conduct data-mining as defined in the *Implementing the Recommendations of the 9/11 Commission Act of 2007, Public Law 110-53, Section 804*? No

29. Will this system have the capability to identify, locate, and monitor individuals or groups of people? No

30. Does Computer matching occur? No

N. ACCOUNTING OF DISCLOSURES

31. 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

31.a. 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

End of Report
