Date of Approval: 09/03/2025
Questionnaire Number: 2558

# Basic Information/Executive Summary

What is the name of your project (system, database, pilot, product, survey, social media site, etc.)?

GSS-21 (Main) | IBM System Z Mainframe Platform zOS System

Acronym:

GSS-21

Business Unit

IT - Cybersecurity

Preparer

# For Official Use Only

Subject Matter Expert

# For Official Use Only

Program Manager

# For Official Use Only

Designated Executive Representative

# For Official Use Only

Executive Sponsor

# For Official Use Only

Executive Summary: Provide a clear and concise description of your project and how it will allow the IRS to achieve its mission.

GSS-21 is an Internal Revenue Service (IRS), Cybersecurity infrastructure support information system that has been categorized as a General Support System (GSS). GSS-21 is comprised of the IRSs IBM System z processing infrastructure and is housed in separate locations. Historically, there are four primary systems running on those devices and they include: 1) Masterfile System 2) 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. 3) Security and Communication System (SACS) 4) 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 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. GSS-21 IBM System Z Mainframe Platform z/OS System has been identified as capturing device identifiers during system operation. These device IDs were not documented in PCLIA 1608. To ensure accuracy and compliance, this newly identified information has now been included within the Personally Identifiable Information (PII) Details section of this assessment.

# Personally Identifiable Information (PII)

Will this project use, collect, receive, display, store, maintain, or disseminate any type of Sensitive but Unclassified (SBU), Personally Identifiable Information (PII), or Federal Tax Information (FTI)?

Yes

Please explain in detail how this project uses sensitive data from inception to destruction (data lifecycle).

SSN's, being unique taxpayer ID numbers, are collected by the applications that run on the infrastructure and stored on the infrastructure. This information is used by the system 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 to enforce laws pertaining to various forms of money laundering.

Please select all types of Sensitive but Unclassified data (SBU)/Personally Identifiable Information (PII)/Federal Tax Information (FTI) that this project uses.

Address
Adoption Taxpayer Identification Number

Agency Sensitive Information
Alien Registration Number
Centralized Authorization File (CAF)
Citizenship or Migration Status
Criminal Investigation Information
Document Locator Number (DLN)
Driver's License Number
Email Address
Employer Identification Number
Employment Information
Family Members
Federal Tax Information (FTI)
Financial Account Number
Individual Taxpayer Identification Number (ITIN)
Name
Official Use Only (OUO) or Limited Office Use (LOU)
Other
Passport Number
Preparer Taxpayer Identification Number (PTIN)
Professional License Number
Protected Information
Social Security Number (including masked or last four digits)
Standard Employee Identifier (SEID)
Tax ID Number
Telephone Numbers

Please explain the other type(s) of PII that this project uses.
Device IDs

Cite the authority for collecting SBU/PII/FTI (including SSN if relevant).
Information by CI for certain money laundering cases - 18 USC
PII about individuals for Bank Secrecy Act compliance - 31 USC
PII for federal tax administration - generally IRC Sections 6001 6011 or 6012
PII for personnel administration - 5 USC
SSN for personnel administration IRS employees - 5 USC and Executive Order 9397
SSN for tax returns and return information - IRC section 6109

# Product Information (Questions)

1 Is this PCLIA a result of a specific initiative or a process improvement?
No

1.1 What is the name of the Business Unit (BU) or Agency initiative?
IT- Cybersecurity

2 What type of project is this (system, project, application, database, pilot/proof of concept/prototype, power platform/visualization tool)?

System

3 What Tier designation has been applied to your system? (Number)

1

4 Is this a new system?

No

4.1 Is there a previous Privacy and Civil Liberties Impact Assessment (PCLIA) for this project?

Yes

4.11 What is the previous PCLIA number?

1608

4.12 What is the previous PCLIA title (system name)?

GSS-21 (Main) | IBM System Z Mainframe Platform

4.2 You have indicated this is not a new system; explain what has or will change and why. (Expiring PCLIA, changes to the PII or use of the PII, etc.)

Updated contact names and the type of PII collected and identified Splunk as the downstream audit logging system.

5 Is this system considered a child system/application to another (parent) system?

No

6 Indicate what OneSDLC State is the system in (Allocation, Readiness, Execution) or indicate if you go through Information Technology's (IT) Technical Insertion Process and what stage you have progressed to.

Execution

7 Is this a change resulting from the OneSDLC process?

No

8 Please provide the full name and acronym of the governance board or Executive Steering Committee (ESC) this system reports to.

IT Cybersecurity Security Operations and Standards Division (SOSD)

9 If the system is on the As-Built-Architecture (ABA), what is the ABA ID number of the system? If this PCLIA covers multiple applications shown on the ABA, please indicate the ABA ID number(s) for each application covered separated by a comma. If the system is not in the ABA, then contact the ABA (https://ea.web.irs.gov/aba/index.html) for assistance.

This system is not on the As-Built-Architecture.

10 If this system discloses any PII to any third party outside the IRS, 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?

Yes

11 Does your project/system involve any use of artificial intelligence (AI), including virtual assistant, chat bot, and robotic process automation, as defined in Executive Order 13960 and 14110?

No

12 Does this system use cloud computing?

No

12.2 Does the CSP allow auditing?

No

13 Does this system/application interact with the public?

No

13.1 If the system requires the user to authenticate, was a Digital Identity Risk Assessment (DIRA) conducted?

No

13.11 Please upload the approved DIRA report using the Attachments button. Select "Yes" to indicate that you have or will upload the signed DIRA form.

No

13.2 If individuals do not have the opportunity to give consent to collect their information for a particular use, why not?

Individuals do not have the opportunity to give consent to collect their information because taxpayer data is required to be collected when filling taxes to be compliant with all US tax code obligations.

13.3 If the individual was not notified of the following items prior to the collection of information, why not? 1) Authority to collect the information 2) If the collection is mandatory or voluntary 3) The purpose for which their information will be used 4) Who the information will be shared with 5) The effects, if any, if they don't provide the requested information.

Individuals do not have the opportunity to give consent to collect their information because taxpayer data is required to be collected when filling taxes to be compliant with all US tax code obligations.

13.4 If information is collected from third-party sources instead of the individual, please explain your decision.

Not Applicable. We do not collect information from third party sources.

14 Describe the business process allowing an individual to access or correct their information. (Due Process)

Individuals do not have access to correct their information using this system.

15 Is this system owned and/or operated by a contractor?

No

15.1 If a contractor owns or operates the system, does the contractor use subcontractors; or do you require multiple contractors to operate, test, and/or maintain this system?

No

16 Identify what role(s) the IRS and/or the contractor(s) performs; indicate what access level (to this system's PII data) each role is entitled to. (Include details about completion status and level of access of the contractor's background investigation was approved for.)

The level of access allowed for each user is determined by the access they are approved for in the Business Entitlement Access Request System (BEARS). Users are only given the access needed to perform their required work. This is known as Role Based access and uses the concept of least privilege.

17 The Privacy Act of 1974 (5 USC § 552a(e)(3)) requires each agency that maintains a system of records, to inform each individual requested to supply information about himself or herself. Please provide the Privacy Act Statement presented by your system or indicate a Privacy Act Statement is not used and individuals are not given the opportunity to consent to the collection of their PII.

A Privacy Act Statement is not used, and individuals are not given the opportunity to consent to the collection of their PII.

18 How many records in the system are attributable to IRS Employees? Enter "Under 50,000", "50,000 to 100,000", "More than 100,000" or "Not Applicable".

Under 50,000

19 How many records in the system are attributable to contractors? Enter "Under 5,000", "5,000 to 10,000", "More than 10,000" or "Not Applicable".

Under 5,000

20 How many records in the system are attributable to members of the public? Enter "Under 100,000", "100,000 to 1,000,000", "More than 1,000,000" or "Not applicable".

More than 10,000

21 Identify any "other" records categories not attributable to the categories listed above; identify the category and the number of corresponding records, to the nearest 10,000; if no other categories exist, enter "Not Applicable".

10,000

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

GSS-21 system access is requested via an Online Form submitted through the Business Entitlement Access Request System (BEARS) application. Access is granted on a need-to-know basis. The 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 system. Deletion from the active access role is also performed through the BEARS application. This control is enforced by Resource Access Control Facility (RACF) Security settings on the user's account.

23 Is there a data dictionary on file for this system? Note: Selecting "Yes" indicates an upload to the Attachment Section is required.

No

24 Explain any privacy and civil liberties risks related to privacy controls.

GSS-21 currently has 25 open findings on the system. These weaknesses have been identified through various means including Security Assessment Reports (SAR) findings, Qualys network vulnerability scans, Guardium DB2 scans and GAO/TIGTA audits. These findings are documented in the Assessment, Authorization, and Risk Governance (AARG) system with Plans of Action and Milestones (POA&Ms) which describe in detail what the finding is, when and how it was discovered and a planned remediation date with milestones. A listing of the POA&Ms is attached to this PCLIA.

25 Please upload all privacy risk finding documents identified for the system (Audit trail, RAFT, POA&M, Breach Plan, etc.); click "yes" to confirm upload(s) are complete.

Yes

26 Describe this system's audit trail in detail. Provide supporting documents.

Auditing is done through the collection of System Management Facilities (SMF) records which document all user activity such as login, logoff, successful and unsuccessful access attempts and any other action a user takes while using the system. These SMF records are captured and initially stored in Generation Data Group (GDG) datasets. They are later stored using virtual tape until the end of the retention period is reached at which time the GDG's are automatically deleted from storage. These SMF records are uploaded to Splunk, which is the official downstream audit logging system for the mainframes.

27 Does this system use or plan to use SBU data in a non-production environment?

Yes

# Interfaces

**Interface Type**

IRS Systems, file, or database

Agency Name

U.S. Department of Education

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Secure File Transfer Protocol (SFTP)

**Interface Type**

IRS Systems, file, or database

Agency Name

Splunk

Incoming/Outgoing

Both

Transfer Method

Secure File Transfer Protocol (SFTP)

**Interface Type**

IRS Systems, file, or database

Agency Name

Centers for Medicare & Medicaid Services (CMS)

Incoming/Outgoing

Outgoing (Sending)

Transfer Method

Secure File Transfer Protocol (SFTP)

**Interface Type**
IRS Systems, file, or database
Agency Name
Railroad Retirement Board
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Secure File Transfer Protocol (SFTP)

**Interface Type**
IRS Systems, file, or database
Agency Name
The Department of the Treasury Bureau of the Fiscal Service
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Secure File Transfer Protocol (SFTP)

**Interface Type**
IRS Systems, file, or database
Agency Name
Social Security Administration & U.S. Department of Health and Human Services Administration for Chi
Incoming/Outgoing
Outgoing (Sending)
Transfer Method
Secure File Transfer Protocol (SFTP)

# Systems of Records Notices (SORNs)

**SORN Number & Name**
Treasury .009 - Treasury Financial Management Systems
Describe the IRS use and relevance of this SORN.
This SORN allows the Treasury Department and the IRS to disclose information to organizations outside of the Treasury Department. This includes organizations such as the Department of Justice, Federal, State, local, or foreign agencies, Congressional Offices, news media, etc.

SORN Number & Name
IRS 24.046 - Customer Account Data Engine Business Master File

Describe the IRS use and relevance of this SORN.

To maintain records of business tax returns, return transactions, and authorized taxpayer representatives.

**SORN Number & Name**

IRS 24.030 - Customer Account Data Engine Individual Master File

Describe the IRS use and relevance of this SORN.

To maintain records of tax returns, return transactions, and authorized taxpayer representatives.

**SORN Number & Name**

IRS 34.037 - Audit Trail and Security Records

Describe the IRS use and relevance of this SORN.

To identify and track any unauthorized accesses to sensitive but unclassified information and potential breaches or unauthorized disclosures of such information or inappropriate use of government computers to access Internet sites for any purpose forbidden by IRS policy (e.g., gambling, playing computer games, or engaging in illegal activity), or to detect electronic communications sent using IRS systems in violation of IRS security policy.

# Records Retention

What is the Record Schedule System?

General Record Schedule (GRS)

What is the retention series title?

GENERAL RECORDS SCHEDULE 3.2: Information Systems Security Records

What is the GRS/RCS Item Number?

31

What type of Records is this for?

Both (Paper and Electronic)

Please provide a brief description of the chosen GRS or RCS item.

This GRS item provides guidelines for record retention related to system users. This includes information related to items such as user profiles, log-in activities, passwords, audit trail files and extracts, system usage files and cost-back files used to assess charges for system use.

What is the disposition schedule?

Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

# Data Locations

What type of site is this?

System

What is the name of the System?

GSS-21 (Main) | IBM System Z Mainframe Platform

What is the sensitivity of the System?

Federal Tax Information (FTI)

Please provide a brief description of the System.

GSS-21 provides the infrastructure that IRS applications use to collect and process taxpayer data. IBM mainframes are located at the Enterprise Computing Centers in XXXXXXXXXXX, XX and XXXXXXX, XX.

What are the incoming connections to this System?

The IRS has service level agreements and memorandums of understanding (SLA's/MOU's) with several other government agencies. These SLAs and MOUs are listed elsewhere in the PCLIA. These documents allow for the transfer of data between these agencies.

What are the outgoing connections from this System?

The IRS has service level agreements and memorandums of understanding (SLA's/MOU's) with several other government agencies. These SLAs and MOUs are listed elsewhere in the PCLIA. These documents allow for the transfer of data between these agencies.