Date of Approval: **November 01, 2021**

PIA ID Number: **6512**

SYSTEM DESCRIPTION

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

General Support System GSS-24 UNIX (Tier 1), GSS-24 UNIX (Tier 1)

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?

GSS-24 UNIX, PIA 4584

What is the approval date of the most recent PCLIA?

12/18/2019

Changes that occurred to require this update:

Significant System Management Changes

Were there other system changes not listed above?

Yes

What were those changes?

The boundary for GSS-24 has changed, entailing the International Business Machine (IBM) Advanced Interactive eXecutive (AIX), Websphere, WebLogic and Apache components have moved under a different GSS. Oracle Application Server is now called Oracle Fusion Middleware and it has also moved to a different GSS and Solaris 9 has retired.

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

Enterprise Operations Governance Board (GB)

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-24 is comprised of the UNIX systems housed in Enterprise Computing Center-Memphis (ECC-MEM), Enterprise Computing Center-Martinsburg (ECC-MTB), and Ogden, UT within Enterprise Operations. The Information Technology (IT) Infrastructure Division is responsible for deploying and maintaining the hardware and software configurations that the Enterprise Computing Centers manage on a day-to-day basis for the UNIX environment. GSS-24 systems operate on Solaris operating systems. The Oracle Database Management System is used by applications hosted on the GSS. GSS-24 servers support Production/Pre-prod and Disaster Recovery (DR) environments. Applications only reside on the UNIX Servers and are not part of the GSS-24 boundary. The UNIX based test/development servers are supported by GSS-27 and are within the boundary of GSS-27.

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:

Security Background Investigations

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

Delivery of governmental benefits, privileges, and services

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

There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed. There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system.

Describe the planned mitigation strategy and forecasted implementation date to mitigate or eliminate the use of SSN's (or tax identification numbers).

There is no alternative to the use of the SSN. The SSN is the significant part of the data being processed. There is no planned mitigation strategy to mitigate or eliminate the use of the SSN on the system.

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:

Mailing address
Date of Birth
Standard Employee Identifier (SEID)
Tax Account Information

Does this system use, collect, receive, display, store, maintain, or disseminate SBU information that is not PII?

No

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.

GSS-24 contains UNIX servers and databases that provide infrastructure support for the applications that are hosted on the GSS. The only data maintained by the GSS on the components consist of configuration settings and audit logs to monitor all administrative actions. The business need for requesting the SEID is to provide accountability for the actions performed by the GSS users for their access to systems.

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

The SEID is issued to the IRS employee by GSS-17. When the user logs into the system with their SEID and password, if the combination is incorrect, the user will not be authorized to access the systems.

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 34.037 Audit Trail and Security Records

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

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?

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.

Notice, consent, and due process are addressed by the individual UNIX systems that make up GSS-24.

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

No

Why not?

Notice, consent, and due process are addressed by the individual UNIX systems that make up GSS-24.

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

Notice, consent, and due process are addressed by the individual UNIX systems that make up GSS-24.

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

IRS Contractor Employees

Contractor Users: Read Write

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

Access to audit login information is restricted to Cybersecurity Operations. Audit logs are sent to the group for review and analysis. Access to the data is determined by the manager based on a user's position and need-to-know. The manager will request a user to be added. They must submit the request via Online 5081/ (Business Entitlement Access Request System (BEARS) to request access to the system.

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.

UNIX Platform - General Support System GSS-24 is non-record keeping. GSS-24 provides network infrastructure and platform support to applications hosted on the GSS servers. It is not a data repository system. Audit trail elements comply with IRM 10.8.3, Audit Logging Security Standards and are maintained in accordance with General Records Schedule (GRS), Document 12829, 3.2, Item 030. Audit logs are approved for deletion/destruction when an agency has determined they are no longer needed for administrative, legal, audit, or other operational purposes. IRS audit data and audit logs are passed to the Security Audit and Analysis System (SAAS) where it is maintained for seven years (in accordance with NARA Job No. N1-58-10-22, approved 4/5/2011). SAAS disposition instructions are published in IRS Document 12990, Records Control Schedule 19 for Enterprise Computing Center - Martinsburg, item 88.

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?

3/3/2021

Describe the system's audit trail.

Physical and logical access controls are in place to restrict access to the PII data to authorized users only. The physical sites where the equipment resides is in compliance with the physical security controls mandated by National Institute of Standards and Technology (NIST). Only authorized Cybersecurity Operations have access to the audit logs stored on the servers. Once the audit logs are moved to backup tapes, they are stored encrypted.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

GSS-24 has a System Security Plan and Information System Contingency Plan. We are not required to have a Security Test Plan. GSS systems do not conduct application-like development. IRS GSS systems are mainly made up 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?

Yes

Describe the type of information derived from these efforts and the technical (e.g., audit trails) or other processes used to limit unauthorized monitoring.

IRS Enterprise Continuous Monitoring procedures are in place for the GSS. These procedures are completed annually to ensure the application and its data are properly secured. In addition, the Application Annual Security Control Assessment (ASCA) process is completed every three years or when a significant change is made to the system.

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