Date of Approval: February 1, 2017 PIA ID Number: **2000**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. GSS-24 UNIX, GSS-24

2. Is this a new system? No

2a. If **no**, is there a PIA for this system? Yes

If **yes**, enter the full name, acronym, PIA ID Number and milestone of the most recent PIA.

1615 and 642

Next, enter the **date** of the most recent PIA. 1/13/2016

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

No	**Addition of PII**
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**

Were there other system changes not listed above? Yes

If yes, explain what changes were made. GSS-31 merged with GSS-24.

3. Check the current ELC (Enterprise Life Cycle) 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**
No	**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-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 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. The applications are supported by Web server software including IBM WebSphere and Oracle Application Server. Oracle Application Server is in process of being replaced with Oracle WebLogic Web server software. The deployment of Oracle WebLogic initiated in early 2011 and is currently being deployed across the GSS. This GSS includes servers supporting Production/Pre-prod/DR-prod/dev environment and applications residing on the on these UNIX Servers. All other UNIX test/dev servers are supported by GSS-27. The boundary for GSS-24 includes: •Operating Systems: Solaris v9 and v10 (SSP-Main) •Oracle Database: Oracle Database v10g and v11g (SSP-App M) •Oracle Application: Oracle Application Server v10gas (SSP-App N) •Web Server Software: IBM WebSphere Application Server v6.1.0.35 to 8.0.0.5 (SSP-App N) •Oracle WebLogic: Oracle WebLogic Application Server v10.x (SSP-App N) used by application within the GSS-24 environment. Applications within GSS-24 includes: •AWSS Employee Connection (EC) •Correspondence Production Services (CPS) •Excise File Information Retrieval System (ExFIRS), Service Center Recognition Image Processing System (SCRIPS) • Tier II Web. These UNIX servers are generally deployed by a Project Office or a Business Unit without the support of the IT Infrastructure Division in Enterprise Operations. Enterprise Computing Center organization or a Business Unit may be responsible for the day-to-day management of these UNIX servers.

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

6a. 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 who the SSN (or tax identification number) is collected on.

Yes On Primary No On Spouse No On Dependent

If **yes**, check all types SSN s (or tax identification numbers) that apply to this system:

Yes	**Social Security Number (SSN)**
No	**Employer Identification Number (EIN)**
Yes	**Individual Taxpayer Identification Number (ITIN)**
No	**Taxpayer Identification Number for Pending U.S. Adoptions (ATIN)**
No	**Practitioner Tax Identification Number (PTIN)**

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 planed mitigation strategy to mitigate or eliminate the use of the SSN on the system.

6b. Does this system contain other (non-SSN) PII that it uses, collects, receives, displays, stores, maintains, or disseminates? (i.e. Names, addresses, etc.) Yes

If **yes**, specify the information.

Selected	PII Element	On Primary	On Spouse	On Dependent
No	Name	No	No	No
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
Yes	Date of Birth	Yes	No	No
No	Place of Birth	No	No	No
Yes	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
No	Internet Protocol Address (IP Address)	No	No	No
No	Criminal History	No	No	No
No	Medical Information	No	No	No
No	Certificate or License Numbers	No	No	No
No	Vehicle Identifiers	No	No	No
No	Passport Number	No	No	No
No	Alien (A-) Number	No	No	No
No	Financial Account Numbers	No	No	No
No	Photographic Identifiers	No	No	No
No	Biometric Identifiers	No	No	No
No	Employment (HR) Information	No	No	No
No	Tax Account Information	No	No	No

6c. Does this system contain SBU information that is not PII, it uses, collects, receives, displays, stores, maintains, or disseminates? No

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

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

No	**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**
No	**PII for personnel administration is 5 USC**
No	**PII about individuals for Bank Secrecy Act compliance 31 USC**
No	**Information by CI for certain money laundering cases may be 18 USC**

6f. 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.

GSS-24 contains UNIX servers, database and web software that provide infrastructure support for the application that are hosted on the GSS. The only date 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 the their access to systems. Some small business employers utilize the SSN.

8. How is the SBU/PII verified for accuracy, timeliness, and completeness? Explain how steps are taken to ensure that all information maintained by the system that is used by IRS to make any adverse determination about an individual's rights, benefits, and/or privileges is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination

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.

C. PRIVACY ACT AND SYSTEM OF RECORDS

9. Are 10 or more records containing SBU/PII maintained, stored, and/or transmitted by or through this system? Yes

9a. If **yes**, are records in the system retrieved by any personal identifier (e.g., name, SSN, Photograph, IP Address) for an individual? Yes

If **yes**, is there a System of Records Notice(s) or SORNs that addresses the PII records in this system? Yes

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

SORNS Number	SORNS Name
Treas/IRS 34.037	**IRS Audit Trail and Security Records System**
Treas/IRS 24.030	**IMF**
Treas/IRS 24.048	**BMF**

If **yes**, does the System of Records Notice(s) (SORN) published in the Federal Register adequately describe the records as required by the Privacy Act? Yes

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. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? 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, cloud, global position system (GPS), biometrics, 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/is notice provided to the individual prior to collection of information? No

17b. If **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.

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

18b. If no, why not? Notice, consent, and due process are addressed b the individual UNIX systems that make up GSS-24.

19. 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.

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

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

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? Access to audit login formation 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 O5081 process to request access to the system.

21b. If computer matching occurs, can the business owner certify that it meets requirements of IRM 11.3.39 Disclosure of Official Information, Computer Matching & Privacy Protection Act ? Yes

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

22a. 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.

UNIX Consolidated Platform - General Support System GSS-24 is non-recordkeeping. GSS-24 provides network infrastructure and platform support to applications hosted on the GSS. 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.

I.2 SA&A OR ECM-R

23. Has the system been through SA&A (Security Assessment and Authorization) or ECM-R (Enterprise Continuous Monitoring Reauthorization)? Yes

23a. If **yes**, what date was it completed? 5/2/2016

23.1 Describe in detail 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 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.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? No

24c. If **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 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

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:

26a. IRS Employees: Under 50,000
26b. Contractors: Under 5,000
26c. Members of the Public: Not Applicable
26d. Other: No

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 9/11 Commission Recommendations 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? Yes

If **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.

N. ACCOUNTING OF DISCLOSURES

30. 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

End of Report