Date of Approval: June 24, 2016 PIA ID Number: **1754**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Enterprise LINUX Platform, GSS-42

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.

GSS-42 Enterprise LINUX Platform # 464

Next, enter the **date** of the most recent PIA. 8/6/2013

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

No 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. All Test/Dev servers moved to GSS-27

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-42 is comprised of the Redhat Enterprise Linux/zLinux (RHEL) Platform systems. 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 Enterprise Linux Platform environment. This GSS includes servers supporting the production environments for Enterprise Linux Platform. The GSS ONLY provides infrastructure for the support of Enterprise Tax Administration and Administrative Support Applications. This GSS includes JavaBeans Open Sources Software Application Server (JBOSS) Enterprise Application Platform. The mandate to develop applications using more Commercial-Off-the-Shelf (COTS) means more IRS applications written in Java and using the JBOSS Enterprise Application Platform (EAP) as the middleware to build and manage enterprise Java applications." Currently, Linux/zLinux platforms supporting ACA and Enterprise "Tools" are not included in this boundary. The Oracle Database Management System is used by applications hosted on the GSS. Oracle Application Server is in process of being replaced with Oracle WebLogic Web server software. The deployment of Oracle WebLogic was initiated in early 2011 and is currently being deployed across the GSS. GSS-27 is integral in supporting the development and testing of Linux/zLinux infrastructure applications prior to their submission into the production environment. GSS-42 includes the following elements: -RHEL Operating System v5 and v6: The operating system for all GSS-42 physical and virtual servers including IBM Mainframe virtual servers in production. -Oracle Database v11g: The database management system used to support GSS-42 components. -Red Hat JBoss EAP v5.1.2: Middleware used to build, deploy, and host enterprise Java applications and services. -Red Hat JBoss EAP v6.x: Middleware used to build, deploy, and host enterprise Java applications and services.

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 planned 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-42 is comprised of the Redhat Enterprise Linux/zLinux (RHEL) Platforms. 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 Enterprise Linux Platform environment.

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. Then 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 system. The GSS utilizes the Enterprise Remote Access Project to control all methods of secure remote access into the IRS network.

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**
34.037	IRS Audit Trail and Security Records System

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. ## Redacted Information For 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 LINUX platforms that make up GSS-42. Due Process is provided pursuant to 5 USC.

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 by the individual LINUX platforms that make up GSS-42. Due Process is provided pursuant to 5 USC.

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 LINUX platforms that make up GSS-42. Due Process is provided pursuant to 5 USC.

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	Read and Write
Developers	No	

Contractor Employees? Yes

Contractor Employees?	Yes/No	Access Level	Background Invest.
Contractor Users	Yes	Read-Only	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 log information is restricted to CyberSecurity Operations. Audit logs are sent to this group for review and analysis. Access to the data is determined by the manager based on the user's position and need-to-know. The manager will request a user to be added. They must submit the request via the Online 5081 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.

The Enterprise LINUX Platform General Support System (GSS-42) is non-recordkeeping. GSS-42 provides network infrastructure and platform support for systems that the Enterprise Computing Centers support/manage for the Enterprise Linux Platform environment. Each recordkeeping application residing on GSS-42 has/will have its own retention period. Audit logs may be retained up to seven (7) years, per IRM 1.15. All systems that contain audit log information are protected from unauthorized access, modification and deletion by limiting the associated user accounts to only authorized personnel. Access to operating system audit logs is strictly controlled and limited to system administrators. Audit logs are protected by strong access controls to help prevent unauthorized access to ensure events are not overwritten. Access to on-line audit logs is strictly controlled. Audit logs are protected by strong access controls to help prevent unauthorized access to ensure events are not overwritten. At the end of the retention period, the audit logs are reviewed to determine if the logs require archival at the Federal Records Center or destruction. Additional guidance is provided in IRM 1.15.

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 systems 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 the National Institute of Standards and Technology. 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-42 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. GSS-42 has taken a Risked Based Decision for this control. EO-RBD-2014-420

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 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