Date of Approval: August 12, 2016 PIA ID Number: **1757**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. Affordable Care Act (ACA) LINUX Platform, GSS-41

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.

463 Affordable Care Act (ACA) LINUX Platform, GSS-41

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? No

.

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
Yes	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.

The Patient Protection and Affordable Care Act (PPACA) contains tax revenue provisions that will need to be implemented within the Internal Revenue Service (IRS). The ACA LINUX Platform General Support System (GSS-41) is the IRS given boundary for the health care system task. Users of GSS-41 components use an Identification and Authentication process to access the different systems. GSS-41 is the infrastructure support for ACA Applications, GSS-41 includes servers supporting production for the Linux ACA environment.

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.)? No

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
No	Mailing address	No	No	No
No	Phone Numbers	No	No	No
No	E-mail Address	No	No	No
No	Date of Birth	No	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? Yes

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

Selected	SBU Name	SBU Description
No	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.
No	Proprietary data	Business information that does not belong to the IRS
No	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
Yes	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.

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
No	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
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.

Section 208 of the E-Government Act of 2002 and Section 522 of the Consolidated Appropriations Act of 2005 require that when developing or procuring systems or projects that collect, use, store, and/or disclose information in identifiable form from or about members of the public or agency employees [the latter prescribed by Sect. 522], to identify potential privacy risks and implement appropriate privacy controls and compliance requirements. GSS-41 does contain privacy information as system administrators and database administrators use the SEID for login. GSS-41 and its components do not collect or process data, however the GSS-41 provides infrastructure services to ACA-IS IRS applications that contain PII. The GSS utilizes the Enterprise Remote Access Project (ERAP) to control all methods of secure remote access into the IRS network. Users of GSS-41 components use their assigned SEID as part of the Identification and Authentication to access the OS, DBMS, JBoss and webMethods components.

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

SEIDs are granted by HR. HR has the responsibility for managing all SEIDs. When the user logs in to the system with their SEID and password, if the combination is incorrect, the user will not be authorized to access the system 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
Treas/IRS 24.030	IMF
Treasury/IRS 24.046	Customer Account Data Engine Business Master File

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.
Not Applicable, notice, consent, and due process are addressed by the individual LINUX platforms that make up GSS-41. 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? Not Applicable, notice, consent, and due process are addressed by the individual LINUX platforms that make up GSS-41. 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?
Not Applicable, notice, consent, and due process are addressed by the individual LINUX platforms that make up GSS-41. 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? 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. Users of GSS-41 components use their assigned SEID as part of the Identification and Authentication to access the OS, DBMS, JBoss, and webMethods components

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 ? Not Applicable

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 ACA LINUX Platform General Support System (GSS-41) is scheduled. As a General Support System under the umbrella of The Treasury FISMA Inventory Management System (TFIMS); GSS-41 data, procedures, and documentation are covered under Records Schedule DAA-0056-2012-0002, as United States Department of the Treasury FISMA Inventory Management System (TFIMS) Media Neutral. Backup tapes are properly scheduled under General Records Schedule (GRS) 3.2, Item 040, and audit trails are properly scheduled under General Records Schedule (GRS) 3.2, Item 031. Each recordkeeping application residing on GSS-41 has/will have its own retention period. Audit logs may be retained up to seven (7) years, per 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? 6/29/2015

23b. If **in process**, when is the anticipated date of the SA&A or ECM-R completion?

23c. If **no**, is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

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. Employee Login data is collected and stored as an auditable event as part of the underlying OS, DBMS, JBoss, or webMethods component. GSS-41 does not have an approved audit plan, but will utilize the associated approved Platform Level Audit Plans for each component to identify specific data elements. 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.

J. PRIVACY TESTING

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

24c. If **no**, please explain why. GSS-41 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

If **yes**, provide a citation and/or link to the most recent Treasury data-mining report to Congress in which your system was discussed (if applicable).

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 (ECM) 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 Controls 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