NOTE: The following reflects the information entered in the PIAMS website.

Date of Submission: December 7, 2015 PIA ID Number: **1459**

A. SYSTEM DESCRIPTION

1. Enter the full name and acronym for the system, project, application and/or database. IRS Integrated Enterprise Portals , IEP

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.

IRS Integrated Enterprise Portals (IEP), Registered User Portal (IEP-RUP) Transition component,MS 4b

Next, enter the **date** of the most recent PIA. 7/25/2013

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

Yes	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
No	System Deployment/Milestone 5
Yes	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 Integrated Enterprise Portal (IEP) was designed and implemented to modernize the IRS technology platform with a fully scalable, managed private cloud capability to provide a consistent, unified customer experience in a cost-effective manner. The IEP delivers web-based services for internal and external users through several integrated sub-components. The Integrated Enterprise Portal- Public User Portal (IEP-PUP) consists primarily of the www.irs.gov website and was created to be the online presence of the Internal Revenue Service (IRS). It is intended to store non-Sensitive But Unclassified (SBU) information that pertains to Treasury Department Publication (TDP) 15-71 regulations, and is the organization's anonymous portal. The core functionality of the components and other key information on the www.irs.gov is as follows: disseminate tax news and information; and electronically support the IRS image and mission. The Integrated Enterprise Portal- Registered User Portal (IEP-RUP) is the technical infrastructure which provides the essential security and technology components required for web access to modernized IRS business applications. The IEP-RUP infrastructure is comprised of a web-enabled, electronic commerce infrastructure that provides secure browser-based application services for tax practitioners and taxpayers. The Integrated Enterprise Portal- Transactional Portal Environment (IEP-TPE) is a technology-infrastructure project that provides the essential security and technology components required for secure structure data exchange between the IRS and the Centers for Medicare and Medicaid Services (CMMS) and external transmitters.

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	Yes	On Spouse	Yes	On Dependent

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

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

SSNs provided from external sources are required to be obtained by applications utilizing the Integrated Enterprise Portal- Registered User Portal (IEP-RUP) infrastructure in order for the applications to appropriately process transactions from external sources. The Integrated Enterprise Portal (IEP) does not have the ability to change any data from an external source that passes through the IEP-RUP infrastructure. This data is not permanently stored in the IEP-RUP environment. The IEP-RUP serves as a pass through for the data to be stored at IRS data centers. The IRS backend applications utilize this data. Integrated Enterprise Portal- Transactional Portal Environment (IEP-TPE) and the International Compliance Management Model - International Data Transfer (ICMM-IDT) handle this PII data in transit

within the IEP environment and do not store this PII information on any persistent storage device during processing.

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
Yes	Name	Yes	Yes	Yes
Yes	Mailing address	No	No	No
No	Phone Numbers	No	No	No
Yes	E-mail Address	No	No	No
Yes	Date of Birth	Yes	Yes	Yes
No	Place of Birth	No	No	No
No	SEID	No	No	No
No	Mother's Maiden Name	No	No	No
No	Protection Personal Identification Numbers (IP PIN)	No	No	No
Yes	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
Yes	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
Yes	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	Information designated as OUO or LOU is information that: is

	(OUO) or Limited Official Use (LOU)	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
Yes	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
No	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
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.

SBU/PII provided from external sources are required to be obtained by applications utilizing the IEP-RUP infrastructure in order for the applications to appropriately process transactions from external sources. IEP does not have the ability to change any data from an external source that passes through the IEP-RUP infrastructure. This data is not permanently stored in the IEP-RUP environment. The IEP-RUP serves as a pass through for the data to be stored at IRS data centers. The IRS backend applications utilize this data. IEP-ACA TPE and ICMM-IDT handle this PII data in transit within the IEP environment and do not store this PII information on any persistent storage device during processing.

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 Integrated Enterprise Portal- Public User Portal (IEP-PUP): The SEID and USERIDs are verified for accuracy against the user credentials stored in the IEP Identity and Access Management (IAM) system and any incorrect data is flagged through a ticketing process. Employee e-mail addresses and phone numbers posted through the Content Management System (CMS) are verified and validated through management review process. Any inaccuracies would be noted either by the public and be reported through the Portal Help Desk. Any inaccuracies would be promptly corrected by CMS users. The Integrated Enterprise Portal- Registered User Portal (IEP-RUP): The IEP-RUP components will not process or permanently store PII data. The SEID and USERIDs are verified for accuracy against the user credentials stored in the IEP Identity and Access Management (IAM) system. The IEP-RUP components will temporarily store authorized user transactional data (name, SSN, TIN, Address, Date of Birth). Preparer Tax Identification Number (PTIN) information is not retained in IEP-RUP. However, PTIN information passes through IEP-RUP to an IRS backend server. The IEP-RUP portal application sends a message to the IRS backend which retrieves the file. International Compliance Management Model - International Data Transfer (ICMM-IDT): ICMM-IDT scans incoming files to ensure that it does not contain a malicious payload and then passes it between International Data Exchange Service (IDES) and IRS ICMM FACTA Information Retention (ICMM-FIR). The PII in the information that passes through ICMM-IDT is considered data in transit within the IEP-RUP environment. The Integrated Enterprise Portal-Transactional Portal Environment (IEP-TPE): The SEID and USERIDs are verified for accuracy against the user credentials stored in the IEP Identity and Access Management (IAM) system. The IEP-TPE components will not store PII data at any time on any persistent media.

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
36.003	General Personnel Records
Treas/ IRS 37.111	Preparer Tax Identification Number (PTIN) Records
Treas/IRS 00.001	Correspondence

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. N/A

E. INCOMING PII INTERFACES

11. Does the system receive SBU/PII from other system or agencies? Yes

11a. If **yes**, does the system receive SBU/PII from IRS files and databases? No

11b. Does the system receive SBU/PII from other federal agency or agencies? No

11c. Does the system receive SBU/PII from State or local agency (-ies)? No

11d. Does the system receive SBU/PII from other sources? Yes

If **yes**, identify the source that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
International Data Exchange Service (IDES)	Third party sources	Yes

11e. Does the system receive SBU/PII from **Taxpayer** forms? Yes

If **yes**, identify the forms

Form Number	Form Name
Form 8966	Foreign Account Tax Compliance Act (FATCA) Report

11f. Does the system receive SBU/PII from **Employee** forms (such as the I-9)? No

F. PII SENT TO EXTERNAL ORGANIZATIONS

12. Does this system disseminate SBU/PII? Yes

12a. Does this system disseminate SBU/PII to other IRS Systems? Yes

If **yes**, identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name	Current PIA?	PIA Approval Date	SA & A?	Authorization Date
FATCA ICMM	Yes	04/03/2014	Yes	01/06/2015

Identify the authority and for what purpose? Authority: IEP Authority to Operation (ATO) was signed by Authorizing Official on 30 March 2015. Purpose: The IEP provides the infrastructure for one-stop, Web-based services with the long-term goal of providing a virtual tax assistance center for internal and external users. This investment enables landing page access to services for taxpayers, businesses, practitioners, electronic return originators and IRS employees. Services enabled by the IEP include easy access to forms and publications, electronic payment transactions, delivery of transcripts, tracking of refunds and amended returns, modernized e-filing, free-file for certain classes of taxpayers, and other electronic services. Ensures the public has access to IRS information that is current and accurate with near real-time updates of more than 110,000 forms, publications, news items, rules, and articles. Supports tax preparer agencies or agent's submissions and reduces paper and person-to-person delays between the IRS and the public to complete a tax transaction. Enables taxpayers and tax preparers to easily find and obtain information and material without calling the IRS. Keeps taxpayers' and tax preparers' information secure at a very high protection level.

12b . Does this system disseminate SBU/PII to other Federal agencies? Yes

If **yes** identify the full names of the federal agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) / Memorandum of Understanding (MOU)

Organization Name	Transmission method	ISA/MOU
Centers for Medicare and Medicaid Services	transmit XML data through encrypted tunnels	Yes

Identify the authority and for what purpose? Authority: IEP Authority to Operation (ATO) was signed by Authorizing Official on 30 March 2015. Purpose: The IEP provides the infrastructure for one-stop, Web-based services with the long-term goal of providing a virtual tax assistance center for internal and external users. This investment enables landing page access to services for taxpayers, businesses, practitioners, electronic return originators and IRS employees. Services enabled by the IEP include easy access to forms and publications, electronic payment transactions, delivery of transcripts, tracking of refunds and amended returns, modernized e-filing, free-file for certain classes of taxpayers, and other electronic services. Ensures the public has access to IRS information that is current and accurate with near real-time updates of more than 110,000 forms, publications, news items, rules, and articles. Supports tax preparer agencies or agent's submissions and reduces paper and person-to-person delays between the IRS and the public to complete a tax transaction. Enables taxpayers and tax preparers to easily find and obtain information and material without calling the IRS. Keeps taxpayers' and tax preparers' information secure at a very high protection level.

12c. Does this system disseminate SBU/PII to State and local agencies? No

12d. Does this system disseminate SBU/PII to IRS or Treasury contractors? Yes

If **yes**, identify the contractor source(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name	Transmission method	ISA/MOU
Verizon Managed Security Service (VMSS)/Akamai	IEP connectivity to Akamai and VMSS is restricted and secured. The connection to VMSS is through an active IPSec connection	Yes
International Data Exchange Service (IDES)	Certificate-based mutually authenticated VPN	Yes

Identify the authority and for what purpose? Authority: IEP Authority to Operation (ATO) was signed by Authorizing Official on March 30, 2015. Both Verizon Managed Security Service (VMSS) and Akamai are IEP infrastructure components and documented in detail in the IEP System Security Plan (SSP). Additionally, Akamai received a Provisional Authority to Operate (P-ATO) on August 26, 2013 from the Joint Authorization Board (JAB) of the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a U.S. government-wide program that standardizes the approach to security assessment, authorization and continuous monitoring for cloud products and services. The JAB comprises the Chief Information Officers of the Departments of Defense (DoD) and Homeland Security (DHS) and the General Services Administration (GSA), who lead the management of the program with the National Institute of Standards and Technology (NIST). Foreign Account Tax Compliance Act (FATCA) Purpose: The Integrated Enterprise Portal (IEP) was designed and implemented to modernize the IRS technology platform with a fully scalable, managed private cloud capability to provide a consistent, unified customer experience in a cost-effective manner. The IEP delivers web-based services for internal and external users through several integrated sub-components which enables landing page access to services for taxpayers, businesses, practitioners, electronic return originators and IRS employees. Services enabled by the IEP include easy access to forms and publications, electronic payment transactions, delivery of transcripts, tracking of refunds and amended returns, modernized e-filing, free-file for certain classes of taxpayers, and other electronic services. Ensures the public has access to IRS information that is current and accurate with near real-time updates of more than 110,000 forms, publications, news items, rules, and articles. Supports tax preparer agencies or agent's submissions and reduces paper and person-to-person delays between the IRS and the public to complete a tax transaction. Enables taxpayers and tax preparers to easily find and obtain information and material without calling the IRS. Keeps taxpayers' and tax preparers' information secure at a very high protection level. Akamai is key component of the IEP infrastructure that provides security, availability, and performance benefits to IEP. VMSS provides security services for the real-time analysis of security alerts generated by network hardware and applications. As part of the Foreign Account Tax Compliance Act (FATCA) passed into law, the IRS will require a data exchange service to allow Foreign Financial Institutions (FFIs) and Host Country Tax Administrations (HCTAs) to automatically exchange FATCA data with the United States. The International Compliance Management Model - International Data Transfer (ICMM-IDT) application will meet the data exchange requirement between International Data Exchange Service (IDES), which serves as the Foreign Account Taxpayers portal and IRS ICMM FACTA Information Retention (ICMM-FIR) backend system.

Did the contract include the appropriate 6103(n) clauses for tax return and return information, and Federal Acquisition Regulations privacy clauses?
Yes

12e. Does this system disseminate SBU/PII to other Sources? 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? Yes

17a. If **yes**, how is notice provided? Was the individual notified about the authority to collect the information, whether such is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects, if any, if they decide not to provide any of the requested information?
Individuals are notified via the IRS privacy policy

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

18a. If **yes**, describe the mechanism by which individuals indicate their consent choice(s):
The Integrated Enterprise Portal- Public User Portal (IEP-PUP): The www.irs.gov web pages are the primary source of public tax information. On pages where website visitors voluntarily request information, publications, refund status, or other information, an appropriate application-specific privacy statement is posted. Each statement informs the visitor of the information being requested; why it is being requested; how it will be used and maintained; and, the impact if the information requested is not provided. Each page of IRS.gov provides a link to the IRS Web Privacy Policy as well as links to taxpayers' rights under the Privacy Act and other privacy protection statutes. Departure Notices are available for all viewers when leaving an IRS site.

19. How does the system or business process ensure due process regarding information access, correction and redress? N/A

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)

Contractor 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	No	
Sys. Administrators	No	
Developers	No	

Contractor Employees? Yes

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

21a. How is access to SBU/PII determined and by whom? Individuals access user IDs only when reviewing the audit logs for all components of the IEP. Access to audit logs is restricted to only appropriate individuals to prevent unauthorized deletion or change of audit events. Access to PII information for the entire IEP is based on least privilege and role that the user has on the project. In order to request access to a system that has PII, a user must create a service request in the ticketing system. Upon approval, the system lead will authorize the designated Active Directory system administrator to provision access to the user for the requested system. All access request tickets are monitored and tracked in the ticketing system. When the user no longer requires access to the system, the user or user's team lead will create a service request in the ticketing system to disable the user's access to the system. The FATCA ICMM-IDT solution does not permit system administrators to interact with traffic being validated and does not store PII data within the IEP environment.

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.

IEP recordkeeping data is approved for destruction in accordance with NARA Job No. N1-58-06-1, as approved July 3, 2006, for the "old" Public User Portal (IEP-PUP, IR Web). Final disposition instructions for web content records, as well as management and operations records, are published under Document 12990, item 25 Records Control Schedule for Information Technology. All records housed in the system will be erased or purged from the system at the conclusion of their retention period(s) as required under IRM 1.15.6 Managing Electronic Records. IEP-RUP, to include ICMM-IDT, are non-recordkeeping and do not require any additional scheduling actions. Audit logs, however, are maintained in accordance with General Records Schedule (GRS) 20, Item 1c (published in IRS Document 12829) and will be deleted/destroyed when they are no longer needed for administrative, legal, audit, or other operational purposes. Further guidance for the capture and retention of audit-related records is found in IRM 1.15 and IRM 10.8.3 Audit Logging Security Standards, section 10.8.3.2.2.

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? 2/12/2014

23.1 Describe in detail the system s audit trail. The IEP audit trail capability is documented in detail in the IEP Security Audit Plan. This document and related security documents which contain IEP audit

information are regularly updated and reviewed. Integrated Enterprise Portal (IEP) systems are connected to a centralized log management solution. Auditable events are transmitted via secured connections for real-time analysis of security alerts generated by network devices, hardware and applications. Logs and alerts are analyzed, correlated, classified, and interpreted by security analysts. The collection and management of auditable data complies with IRS, Treasury, and other federal requirements which require the following data elements to be audited: Time stamp (i.e., date and time of the event), Unique identifier (e.g., user name, SID, application name, SEID) of the user or application initiating the event), Type of event (From Auditable Events Table), Subject of event, action taken ("Subject of event" is event specific information varying from source to another, Primarily used by applications (e.g., command code, master file tax (MFT), tax period, Form number), Origin of the request (i.e., terminal ID) for identification/authentication events, Name of object introduced, accessed, or deleted (e.g., specific file, folder), Role of user, when creating the event (e.g., IDRS USR, system administrator, application user), Success or failure of an event, Log on & off to a system, Change of Password, All system administrator (SA) actions, while logged on as a system administrator, Switching accounts or running privileged actions from another account, Creation or modification of supervisor groups, Sub-set of security administrator actions, while logged on in the security administrator role, Sub-set of system administrator actions, while logged on in the user role, Clearing of the audit log file, Startup and shut down of audit functions, Use of identification and authentication mechanisms (e.g., user id and password), Change of file or user permissions or privileges (use of suid/guid, chown, su, etc.), Remote access outside of the corporate network. communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system, Batch file changes made to an application or database, Application critical record changes, Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility), All system and data interactions concerning Taxpayer Data. The help desk Customer Service Representatives (CSRs) and Escalation Specialist records the information for each escalation and thus allows them to provide information in the event of an audit. Note: IEP-TPE AFA follows the same audit procedure as IEP with the addition of logging encrypted LegalName and ETIN.

J. PRIVACY TESTING

24. Does the system require a System Test Plan? Yes

24b. If **yes**, Is the test plan in process or completed: In Process

If **in process**, when is the test plan scheduled for completion? 1/1/2017

24.3 If **completed/ or in process,** describe what testing and validation activities have been conducted or are in progress to verify and validate that the applicable Privacy Requirements (listed in header) have been met?
Tested and validation activities are primarily conducted during through the Annual Security Controls Assessment (ASCA), which tests security and privacy controls.

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: More than 10,000
26c. Members of the Public: More than 1,000,000
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? No

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? Yes

If **yes** , 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? Contact *Disclosure* to determine if an accounting is required. Not Applicable

30b. If **N/A**, explain the Exemption and/or Disclosure s response. The portal does not process returns nor do the contractors or IRS employees in PPMO have access to returns.

End of Report