

Date of Approval: **September 16, 2022**

PIA ID Number: **6800**

SYSTEM DESCRIPTION

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

IRS Integrated Enterprise Portals, IEP

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?

IRS Integrated Enterprise Portals, IEP, # 6249

What is the approval date of the most recent PCLIA?

11/9/2021

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

Significant System Management Changes

Significant Merging with Another System

New Access by IRS employees or Members of the Public

Internal Flow or Collection

Were there other system changes not listed above?

No

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

Infrastructure Executive Steering Committee (IESC)

Current ELC (Enterprise Life Cycle) Milestones:

Detailed Design/Milestone 4A

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.

The Integrated Enterprise Portal (IEP) was designed and implemented to modernize the Internal Revenue Service (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, Public User Portal (IEP-PUP), Registered User Portal (IEP-RUP), Employee User Portal (IEP-EUP), and Transactional Portal Environment (IEP-TPE). IEP was created to support the Information Return Intake System (IRIS) Web Portal and supports additional business needs. The Integrated Enterprise Portal-Public User Portal (IEP-PUP) is the online presence of the IRS, IRS.gov, that allows unrestricted public access to non-sensitive materials and applications, including forms, instructions, news, and tax calculators. No authentication is required for access to any materials on the IEP-PUP. 19 of the 22 PUP Web Applications are deployed within the AWS US GovCloud IaaS. 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 Employee User Portal (IEP-EUP) serves as a pass-through mechanism for web-enabled access for IRS employees and registered users to conduct tax administration transactions through both the portal and Enterprise Application Integration Broker (EAIB) systems. For example, disclosures for third-party income verification using the Income Verification Express Service (IVES), a fully automated verification through the Internet in as close to real-time as practicable. IEP-EUP contains two separate functions, the Customer Service Representative (CSR) Portal and the Business Portal. The Information Return Intake System (IRIS) Web Portal is accessed and allows registered public users to prepare and submit 1099 forms to the IRS through these two input channels (Intake Portal and Application to Application (A2A), which allows IRS employees to view electronic information returns to assist customers with information return questions and also allows for them to correct errors on paper information returns submitted through Service Center Recognition/Image Processing System (SCRIPS). The Business and CSR Portal's will implement solutions for SBSE, customer support representatives and tax examiners. The Integrated Enterprise Portal-Transactional Portal Environment (IEP-TPE) is the technology-infrastructure 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. The Information Return Processing System (IRPS) supports processing of information returns to improve data quality and provides data for assisting downstream compliance systems to identify fraud and assess incorrect information penalties. These services provide validation micro services and batch processes for identity data validation and perfection, improves services for the Affordable Care Act (ACA) and Partnership Bipartisan Budget Act (PBBA) and provides downstream data management with compliance processes. Lastly, the 1099 Form Intake Portal, satisfies the congressional mandate under the "Taxpayer First Act Sec. 2102", which requires provisions to allow taxpayers to electronically file Forms 1099. The system will provide taxpayers with IRS resources and guidance that allows them to prepare, file, and distribute Forms 1099 as well as the ability to create and maintain tax records.

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).

SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. For IVES, the

SSN is required for the transcript disclosure of tax information for third party income verification. The continued use of SSN is needed for CSR due to the Customer service and submission process usage. The IRIS Web Portal requires the use of Social Security Numbers or Employer Identification Numbers because no other identifier can be used to uniquely identify a taxpayer or an organization. SSNs are permissible from the Internal Revenue Code (IRS) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. Based on taxpayer legislation, it requires the collection of PII such as SSN, EIN, and other taxpayer information. The TIN is required to process information returns on the 1099 forms that are submitted on the IRIS Portal.

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

The Office of Management and Budget Circular A-130 requires that federal agencies develop a mitigation or elimination strategy for systems that use SSNs, which the Service continues to develop strategies to meet. An exception to that requirement is when the SSN is uniquely needed to identify a user's record. IEP and its components (Business and Customer Portal's) requires the use of SSNs because no other identifier can be used to uniquely identify a taxpayer at this time. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. 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. SSNs are permissible from Internal Revenue Code (IRC) 6109, which requires individual taxpayers to include their SSNs on their income tax returns. There is currently not a way to eliminate the use of the social security number since it is required for tax reporting purposes.

Employer Identification Number

Other Taxpayer Identification Number

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:

Name
Mailing Address
Phone Numbers
E-mail Address
Date of Birth
Standard Employee Identifier (SEID)
Internet Protocol Address (IP Address)
Medical Information
Vehicle Identifiers

Financial Account Numbers
Employment Information
Tax Account Information
Centralized Authorization File (CAF)

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

Yes

Specify the types of SBU from the SBU Types List:

Agency Sensitive Information Information which if improperly used or disclosed could adversely affect the ability of the agency to accomplish its mission.

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.

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.

Are there other types of SBU/PII used in the system?

Yes

Describe the other types of SBU/PII that are applicable to this system.

Federal Tax Information

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

PII for federal tax administration is generally Internal Revenue Code Sections 6001, 6011, & 6012e(a)

SSN for tax returns and return information is Internal Revenue Code Section 6109

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

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.

SSNs, federal tax information and other SBU/PII provided from external sources are required for use in applications to appropriately process transactions from external sources. The Integrated Enterprise Portal (IEP) delivers services for internal and external users through several integrated sub-components, these include Public User Portal (IEP-PUP), Registered User Portal (IEP-RUP), Employee User Portal (IEP-EUP), and Transactional Portal Environment (IEP-TPE). IEP was created to support the Information Return Intake System (IRIS) Web Portal and supports additional business needs. Taxpayer requests generated in the Integrated Enterprise Portal-Public User Portal (IEP-PUP) come in through IRS.gov; this allows unrestricted public access to non-sensitive materials and applications, including forms, instructions, news, and tax calculators. 19 of the 22 PUP Web Applications are deployed within the AWS US GovCloud IaaS. The Integrated Enterprise Portal-Registered User Portal (IEP-RUP), Employee User Portal (IEP-EUP) serves as a pass-through mechanism for the taxpayer and IRS staff to conduct tax administration transactions through both the portal and Enterprise Application Integration Broker (EAIB) systems, perform disclosures for third-party income verification, ensures an income verification is fully automated and is accomplished through the Internet in as close to real-time as practicable. The Employee Portal is one application with two separate functionalities the Customer Service Representative (CSR) Portal and the Business Portal. IRS employees will view electronic information returns through two input channels Intake Portal and Application to Application (A2A) to assist customers with information return questions. The Business Portal allows IRS Employees to view and correct errors on paper information returns submitted through Service Center Recognition/Image Processing System (SCRIPS). The Integrated Enterprise Portal-Transactional Portal Environment (IEP-TPE) provides the means to secure data; the technology components limits data exchange and provides secure data in transit between the IRS and the Centers for Medicare and Medicaid Services (CMMS) as well as external transmitters. The SBU/PII is used to provide micro services and batch processes for identity data validation and perfection and provides downstream data management to improve compliance processes. Lastly, the 1099 Form Intake Portal, satisfies the congressional mandate under the "Taxpayer First Act Sec. 2102", which requires provisions to allow taxpayers to electronically file Forms 1099. The system will provide taxpayers with IRS resources and guidance that allows them to prepare, file, and distribute Forms 1099 as well as the ability to create and maintain tax records. The IRS backend applications utilize this SBU/PII data via the IRS Integrated Enterprise Portals-Affordable Care Act (IEP-ACA) TPE and ICMM-IDT to securely transfer data within the IEP environment to support MeF transactions. PII is limited to collecting and storing minimal PII from taxpayer records solely for audit and other authorized purposes. The SBU/PII data elements are required in the Business Portal in order to allow IRS employees to view and correct errors on paper information returns submitted through Service Center Recognition/Image Processing System (SCRIPS). SBU/PII information collected in IRIS

Web Portal is viewed through the CSR Portal to allow IRS employees to assist customers with transmitter support. SBU/PII information needs to be collected in order to generate a 1099 Form for the IRIS system.

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

In the Integrated Enterprise Portal-Public User Portal (IEP-PUP), the Single Employee Identification (SEID) and User Identifications (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 email 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 SEID and USERIDs are verified for accuracy against the user credentials stored in the IEP Identity and Access Management (IAM) system. The Employee Portal leverages Information Return Intake Service (IRIS) for validation and completeness and is deemed reliable and accurate. The information is not altered in any way. The Secure Access Digital Identity (SADI) solution for identifying proofing, authentication, and authorization to reduce the risk of bad actors deliberately filing inaccurate and incomplete Forms 1099, it applies pre-filing data checks so users can avoid formatting errors and other common error types.

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 37.111 Preparer Tax Identification Number Records

IRS 00.001 Correspondence Files and Correspondence Control Files

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 24.046 Customer Account Data Engine Business Master File

IRS 36.003 General Personnel and Payroll Records

IRS 34.037 Audit Trail and Security Records

IRS 22.062 Electronic Filing Records

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?

Yes

Does the system receive SBU/PII from IRS files and databases?

Yes

Enter the files and databases:

System Name: Information Return Processing System (IRPS)

Current PCLIA: Yes

Approval Date: 9/22/2021

SA&A: Yes

ATO/IATO Date: 3/12/2020

System Name: Service Center Recognition Image Processing (SCRIPS)

Current PCLIA: Yes

Approval Date: 11/25/2020

SA&A: Yes

ATO/IATO Date: 4/16/2020

System Name: WebApps Enterprise Service Income Verification Exp (WebApp IVES)

Current PCLIA: Yes

Approval Date: 12/3/2021

SA&A: Yes

ATO/IATO Date: 9/30/2021

System Name: Secure Access Digital Identity (SADI) CSP-ID.me (ID.me)

Current PCLIA: Yes

Approval Date: 1/1/2021

SA&A: No

System Name: Foreign Account Tax Compliance Act (FATCA) Financial Institution (FI) Registration System
Current PCLIA: Yes
Approval Date: 11/8/2019
SA&A: Yes
ATO/IATO Date: 2/20/2021

System Name: Modernized eFile
Current PCLIA: Yes
Approval Date: 2/20/2019
SA&A: Yes
ATO/IATO Date: 4/29/2021

System Name: International Compliance Management Model FATCA (ICMM-FIR)
Current PCLIA: Yes
Approval Date: 10/27/2020
SA&A: Yes
ATO/IATO Date: 8/20/2020

System Name: Information Return Intake System (IRIS) Web Portal
Current PCLIA: Yes
Approval Date: 5/20/2022
SA&A: No

System Name: Secure Access Digital Identity (SADI)
Current PCLIA: Yes
Approval Date: 3/14/2022
SA&A: Yes
ATO/IATO Date: 8/23/3021

Does the system receive SBU/PII from other federal agency or agencies?

No

Does the system receive SBU/PII from State or local agency (-ies)?

No

Does the system receive SBU/PII from other sources?

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: International Data Exchange Service (IDES)
Transmission Method: Third Party Source
ISA/MOU: Yes

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: Form 8966

Form Name: Foreign Account Tax Compliance Act (FATCA) Report

Form Number: Forms 1120, 1120-F, 1120-S

Form Name: Corporation Income Tax Return

Form Number: Form 940

Form Name: Employer's Annual Federal Unemployment (FUTA) Tax Return

Form Number: Form 941

Form Name: Employer's QUARTERLY Federal Tax Return

Form Number: Form 941-PR

Form Name: Employer's QUARTERLY Federal Tax Return (Puerto Rican Version)

Form Number: Form 941-SS

Form Name: Employer's QUARTERLY Federal Tax Return (American Samoa, Guam, the Commonwealth of the Northern Mari

Form Number: Form 943

Form Name: Employer's Annual Federal Tax Return for Agricultural Employees

Form Number: Form 943-PR

Form Name: Employer's Annual Federal Tax Return for Agricultural Employees (Puerto Rican Version)

Form Number: Form 944

Form Name: Employer's Annual Federal Tax Return

Form Number: Form 945

Form Name: Annual Return of Withheld Federal Income Tax

Form Number: Form 1041

Form Name: U.S. Income Tax Return for Estates and Trusts

Form Number: Form 2290

Form Name: Heavy Highway Vehicle Use Tax Return

Form Number: Form 720

Form Name: Quarterly Federal Excise Tax Return

Form Number: Form 8849

Form Name: Claim for Refund of Excise Taxes

Form Number: Forms 990
Form Name: Return of Organization Exempt From Income Tax

Form Number: Form 990-EZ
Form Name: Short Form Return of Organization Exempt From Income Tax

Form Number: Form 990-N
Form Name: Annual Electronic Filing Requirement for Small Exempt Organizations

Form Number: Form 990-PF
Form Name: Return of Private Foundation

Form Number: Form 1120-POL
Form Name: U.S. Income Tax Return for Certain Political Organizations

Form Number: Form 2350
Form Name: Application for Extension of Time to File U.S. Income Tax Return

Form Number: Form 4868
Form Name: Application for Automatic Extension of Time To File U.S. Individual Income Tax Return

Form Number: Form 7004
Form Name: Application for Automatic Extension of Time To File Certain Business Income Tax, Information, and Ot

Form Number: Form 8868
Form Name: Application for Extension of Time To File an Exempt Organization Return

Form Number: Form 1040
Form Name: U.S. Individual Income Tax Return

Form Number: Form 1040-ES
Form Name: Estimated Tax for Individuals

Form Number: Form 1040-SR
Form Name: U.S. Tax Return for Seniors

Form Number: Form 1065
Form Name: U.S. Return of Partnership Income

Form Number: Form 1065-B
Form Name: U.S. Return of Income for Electing Large Partnerships

Form Number: Form 4506-C
Form Name: Request for Transcript of Tax Return

Form Number: Form 1099
Form Name: Miscellaneous Information

Form Number: Form 1096

Form Name: Annual Summary and Transmittal of U.S. Information Returns

Form Number: Form 8809

Form Name: Application for Extension of Time to File Information Returns

Does the system receive SBU/PII from Employee forms (e.g., the I-9)?

No

DISSEMINATION OF PII

Does this system disseminate SBU/PII?

Yes

Does this system disseminate SBU/PII to other IRS Systems?

Yes

Identify the full name and acronym of the IRS system(s) that receive SBU/PII from this system.

System Name: Information Return Intake Service (IRIS)

Current PCLIA: Yes

Approval Date: 5/20/2022

SA&A: No

System Name: WebApps Enterprise Service Income Verification Exp (WebApp IVES)

Current PCLIA: Yes

Approval Date: 9/30/2021

SA&A: Yes

ATO/IATO Date: 9/30/2021

System Name: Secure Access Digital Identity (SADI) CSP-ID.me (ID.me)

Current PCLIA: Yes

Approval Date: 1/1/2021

SA&A: No

System Name: Secure Access Digital Identity (SADI)

Current PCLIA: Yes

Approval Date: 3/14/2022

SA&A: Yes

ATO/IATO Date: 8/23/2021

System Name: International Compliance Management Model FATCA (ICMM-FIR)
Current PCLIA: Yes
Approval Date: 10/27/2020
SA&A: Yes
ATO/IATO Date: 8/20/2020

System Name: Taxpayer Delivery System (TDS) (eServices)
Current PCLIA: Yes
Approval Date: 1/11/6202
SA&A: Yes
ATO/IATO Date: 2/21/2021

System Name: Forms Based Process (FBP) Child to IVES
Current PCLIA: No
SA&A: No

Identify the authority.

Authority and purpose is pursuant to section 6103 (h)(1) of the Internal Revenue Code (IRC).
Authority and purpose is pursuant to section 6103(h)(1) of the Internal Revenue Code (IRC).
IRC 6103(h)(1) provides for disclosure of returns and return information to officers and employees of the Department of the Treasury (including IRS) whose official duties require access for tax administration.

For what purpose?

For tax administration purposes.

Does this system disseminate SBU/PII to other Federal agencies?

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: Centers for Medicare and Medicaid Services
Transmission Method: transmit XML data through encrypted tunnels
ISA/MOU: Yes

Identify the authority.

Authority and purpose is pursuant to section 6103(h) of the Internal Revenue Code (IRC) and I.R.C. §6103(l)(12)(C) Disclosure By Centers For Medicare & Medicaid Services With respect to the information disclosed under subparagraph (B). Authority and purpose is pursuant to section 6103(h)(1) of the Internal Revenue Code (IRC). IRC 6103(h)(1) provides for disclosure of returns and return information to officers and employees of the Department of the Treasury (including IRS) whose official duties require access for tax administration. Authority and purpose is pursuant to section 6103(l) of the Internal Revenue Code (IRC). IRC 6103(l) provides for disclosure of returns and return information for purposes other than

tax administration. Provides federal and state agencies authority to use tax data for non-tax programs. Examples: Eligibility for TANF; SNAP; Medicaid; Veteran's mean-tested pensions and health care; Affordable Health Insurance (ACA); Federal Student Aid; Refund Offset for debt collection & Child Support enforcement

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

SORN- Treasury 00.001, Treasury/IRS 24.030, IRS 24.046, 34.037, 37.111 - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted.

For what purpose?

For tax administration purposes.

Does this system disseminate SBU/PII to State and local agencies?

Yes

Identify the full names of the state and local agency(s) that receive SBU/PII from this system, and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Organization Name: All States
Transmission Method: Electronic Files
ISA/MOU: No

Identify the authority.

Authority and purpose is pursuant to section 6103(d) of the Internal Revenue Code (IRC). IRC 6103(d) provides for disclosure of returns and return information to any state agency, body or commission, or its legal representative charged under the laws of the state with the responsibility for administration of any state tax law. Sharing improves the efficiency of State and local agency tax administration and will generate revenue for the State and local agencies with limited expenditures of resources. According to the Office of Privacy and Disclosure (PGLD), W&I has approved agencies as IVES participants. However, PGLD requires that any all disclosure to state/federal agencies have written, executed data sharing agreements/MOUs, and are working toward getting these in place.

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

SORN- Treasury 00.001, Treasury/IRS 24.030, IRS 24.046, 34.037, 37.111 - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. All other records may be used as described below if the IRS deems that the purpose of the disclosure is compatible with the purpose for which IRS collected the records, and no privilege is asserted.

For what purpose?

For tax administration purposes.

Does this system disseminate SBU/PII to IRS or Treasury contractors?

No

Does this system disseminate SBU/PII to other Sources?

Yes

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

Organization Name: Treasury Inspector General for Tax Administration (TIGTA)

Transmission Method: Secure Data transfer (SharePoint or Email)

ISA/MOU: Yes

Identify the authority.

I.R.C. § 6103(i)(2)(A), I.R.C. § 6103(i)(3)(A) Federal Officers or employees for administration of Federal laws not relating to administration

Identify the Routine Use in the applicable SORN (or Privacy Act exception).

SORN- Treasury 00.001, Treasury/IRS 24.030, IRS 24.046, 34.037, 37.111 - Disclosure of returns and return information may be made only as provided by 26 U.S.C. 6103. (Section 6103(i)(2)(A) and I.R.C. § 6103(i)(3)(A)) To appropriate agencies, entities, and persons when: (a) The IRS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) the IRS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the IRS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with IRS efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

For what purpose?

Preparations for judicial or administrative proceedings, investigations that may result in a proceeding, a grand jury proceeding, disclosure of return information to apprise appropriate officials of criminal or terrorist activities or emergency circumstances, administration of Federal laws not relating to administration or possible violations of federal criminal law.

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.?

Yes

Briefly explain how the system uses the referenced technology.

Internet Protocol version 6 helps people to connect to the Internet by significantly increasing the number of IP addresses; the numeric identifiers that computers use to identify a website, computer, or mobile device, that can be assigned.

Does the system use cloud computing?

Yes

Is the cloud service provider (CSP) Federal Risk and Authorization Management Program (FedRAMP) certified?

Yes

Date Certified.

6/21/2016

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

Yes

Who audits the CSP Data?

3rd Party

What is the background check level required for CSP?

Moderate

Is there a breach/incident plan on file?

Yes

Privacy laws (including access and ownership) can differ in other countries. This cloud will be Continental US (CONUS) only for:

Storage
Transmission
Maintenance

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?

Yes

How is notice provided? Was the individual notified about the authority to collect the information, whether disclosure is mandatory or voluntary, the purpose for which the information will be used, with whom the information may be shared, and the effects on the individual, if any, if they decide not to provide all or any of the requested information?

Individuals are notified via the IRS privacy policy statements. Notice, consent, and due process are provided via the IRS systems and their related tax forms instructions and pursuant to Title 5 USC. The IRS notifies all individuals who file tax returns of such collection via the Privacy Act Notice which provides the legal right to ask for information under Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. Under these sections, response is mandatory. Code section 6109 requires the individual provide an identifying number. The Taxpayer is notified by the mortgage banker that there is a pending request for the release of their tax information. All forms come with instructions on what is required. The information within the Business and CSR Portal's comes from various IRS Systems and forms. Those systems and forms provide the Privacy Act Notice to individuals. The Business and Customer CSR Portal's do not directly provide individuals the opportunity to decline from providing information and/or from consenting to particular uses of the information. Notice, consent, and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC. The notice will be displayed on the unique identifier (UI) prior to data collection for the IRIS application.

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

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. The IVES system will provide the capability via Taxpayer's online account (OLA) to either provide consent or decline the release of requested information. IRIS Web Portal does not directly provide individuals the opportunity to decline from providing information and/ or from consenting to particular use of the information. Notice, consent, and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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

Notice, consent, and due process are provided via the IRS systems and their related tax forms instructions and pursuant to Title 5 USC. Any information collected is done so while carrying out the Internal Revenue laws of the United States. The IVES system will be protected by the appropriate level of Authentication & Authorization services. For the CSR application, after checking status to find out that their submission contains an error or was rejected, the submitter can correct the error(s) in their own environment and re-submit. The rejection response from the IRS to the submitter will include details as to why the submission was rejected. Likewise, in the case of incorrect information that does not cause a reject, the submitter will be informed as to exactly what elements are incorrect. Transmitters will have access to IRS personnel (dedicated phone lines), as well as documentation (published documents as well as material at IRS.gov) to assist them in interpreting the responses, making necessary corrections, and resubmitting the transmission. The IRIS Web Portal provides a correction mechanism for any transmitted data. Additionally, they can contact customer support if they want to dispute any data provided through the system.

INFORMATION PROTECTION

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

The following people have access to the system with the specified rights:

IRS Employees

Users: Read Write

IRS Contractor Employees

Contractor System Administrators: Read Write

Contractor Developers: Read Write

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

Access to the Integrated Enterprise Portals (IEP) is requested via an ERC ticketing process. Access is granted on a need-to-know basis. (Audit logs and/or IEP data) The enrollment process requires that an authorized manager approve access requests on a case-by-case basis. Access approval is based on the Users role(s) and responsibilities. Users are given the minimum set of privileges required to perform their regular and recurring work assignments; they are restricted from changing the boundaries of their access without management approval. The employee's access will be terminated once they no longer require access. Access to Business and CSR Portals are determined by their roles of the employees and maintained through BEARS (Business Entitlement Access Request System) formerly known as OL5081 (system access request), which is approved by managers and system administrators. Access is based on hierarchy roles and permissions. Access to IRIS Portal is determined by the roles of the employees and maintained through BEARS (Business Entitlement Access Request System) formerly known as OL5081 (system access request), which is approved by managers and system administrators. Access is based on hierarchy roles and permissions. The FATCA ICMM-IDT and MeF Resiliency solutions do not permit system administrators to interact with traffic being validated and does not store PII data within the IEP environment. Access to the data is determined by the System Administrator based on a user's position and need-to-know. Contractors, including Developers, will not have direct access to the Two Factor Authentication (TFA) IVES production system or database. Only IRS System Administrators will have access to the production environment. Information requested by the Treasury Inspector General for Tax Administration must be properly vetted and cleared for release.

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.

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, RCS 17, 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) 3.2, Item 030 (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. All records housed in the IVES system will be erased or purged from the system at the conclusion of their retention period(s) as required under Internal Revenue Manual (IRM) 1.15.6. A control log is maintained containing the media label ID, date and method of destruction, and the signature of the person who destroyed the media. 1040X master data file and associated records will be disposed of in accordance with Records Control Schedule (RCS) 29 for Tax Administration-Wage & Investment, Item 55-56. Recordkeeping copies of system data will be destroyed on or after January 16, 6 years after the end of the processing year (Job No. N1-58-95-1). All records housed in the IRIS Web Portal will be erased or purged from the system in accordance with approved retention periods. IRS Web Portal data retention is done in accordance with RCS item 29 and items 85, 87, 88, and 129 in addition to IRM 1.15.6 Managing Electronic Records. All records will be destroyed in accordance with the applicable Records Control Schedules. Audit Records are retained in accordance with GRS 3.2, item 030 and 031.

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?

4/30/2021

Describe the system's audit trail.

The IEP audit trail capability is documented in detail in the IEP System Security 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.

PRIVACY TESTING

Does the system require a System Test Plan?

Yes

Is the test plan completed?

Yes

Where are the test results stored (or documentation that validation has occurred confirming that requirements have been met)?

The test results are stored in Treasury FISMA Inventory Management System (TFIMS). System Administrators performs ongoing system installation, configuration, operation, maintenance, and monitoring, including administration of security controls or security-related components of the system. The annual information system security assessments, including technical control testing and updated risk analyses, are conducted in compliance with Treasury and applicable guidance. System authorizations are conducted and maintained in accordance with IRS-defined policy and frequencies identified in the Federal Information Processing Standards and the National Institute of Standards and Technology and all assessments, results, and reports, stored in Treasury's FISMA Inventory Management System (TFIMS).

Were all the Privacy Requirements successfully tested?

Yes

Are there any residual system privacy, civil liberties, and/or security risks identified that need to be resolved?

No

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?

The Annual Security Controls Assessment (ASCA) conducted by IRS Certification Program Office (CPO).

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: More than 10,000

Members of the Public: More than 1,000,000

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?

No

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?

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.

Yes