

Date of Approval: **December 15, 2021**

PIA ID Number: **6574**

SYSTEM DESCRIPTION

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

Secure Data Transfer - Department of Labor (DOL), SDT

Is this a new system?

Yes

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

Tax Exempt Government Entities Executive Steering Committee (TEGE IESC)

Current ELC (Enterprise Life Cycle) Milestones:

Operations & Maintenance (i.e., system is currently operational)

Is this a Federal Information Security Management Act (FISMA) reportable system?

No

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 purpose of the Secure Data Transfer - DOL system is to transfer pension plan data between the Department of Labor (DOL) and Employee Plans (EP) of the Internal Revenue Services (IRS). The DOL and IRS have a Memorandum of Understanding (MOU) in which they share information concerning Pension Plans. DOL needs tax information (returns, payroll returns, W-2s or information the IRS secured during an examination) to prove an entity or individual was not truthful in their return filings and potentially took pension funds for personal usage. Also, information is needed to verify the individual or entity has financial resources to make the trust and individuals whole. IRS and DOL also transfer referral forms 6212-A (from DOL to IRS) and Form 6212-B (from IRS to DOL).

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:

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

Law enforcement and intelligence purposes

Explain why the authorized use(s) above support the new or continued use of SSNs (or tax identification numbers).

The information is needed in prosecution of individuals or entities.

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

There is no mitigation strategy as Individual SSN's and EIN's are required for identification of the record.

Employer 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
Date of Birth
Tax Account Information

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

No

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.

Sometimes they request workpapers or information collected by the IRS during the course of an audit.

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)

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.

SBU/PII is limited to the name, address, SSN and/or EIN of the organization or taxpayer as listed on the Forms 6212-A or 6212-B. The name, address SSNS and/or EIN are needed for identification purposes.

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

Sources of SBU/PII are from DOL referrals and requests which have been verified by the DOL. Hence, source of information is considered accurate, timely, and complete. IRS will use the leads provided through referrals to perform further research and verification with IRS data to determine audit potential or other appropriate action. Where indicators of non-compliance exist, IRS will take the necessary enforcement actions to ensure compliance.

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 42.021 Compliance Programs and Projects Files

IRS 34.037 Audit Trail and Security 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: Integrated Data Retrieval System (IDRS)

Current PCLIA: Yes

Approval Date: 10/26/2021

SA&A: Yes

ATO/IATO Date: 10/1/2018

System Name: Employee User Portal (EUP)
Current PCLIA: Yes
Approval Date: 10/1/2018
SA&A: No

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

Yes

For each federal interface, identify the organization that sends the SBU/PII, how the SBU/PII is transmitted and if there is an Inter-Agency Agreement (ISA) /Memorandum of Understanding (MOU).

Name: DOL
Transmission Method: SDT-DOL
ISA/MOU: Yes

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

No

Does the system receive SBU/PII from other sources?

No

Does the system receive SBU/PII from Taxpayer forms?

No

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?

No

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: DOL
Transmission Method: SDT
ISA/MOU: Yes

Identify the authority.

MOU with Department of Labor

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

TEGE and DOL have a Memorandum of Understanding with which they share information concerning pension plans. DOL and TEGE are each responsible for ensuring entities are in compliance with various Pension laws and regulations. Information shared between the agencies will be used to assist in their compliance programs and projects.

For what purpose?

Sharing of information so the agency can regulate laws

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

No

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

No

Does this system disseminate SBU/PII to other Sources?

No

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.?

No

Does the system use cloud computing?

No

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?

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.

Information is not collected from individuals; it is obtained from DOL and/or IRS information systems.

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

No

Why not?

Notice, consent, and due process are provided 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 pursuant to 5 USC.

INFORMATION PROTECTION

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

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

IRS Employees

Users: Read Write

Managers: Read Write

System Administrators: Administrator

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

"The Secure Data Transfer - DOL, SDT system is located on a secure server; each user must obtain permission to access the server folder to be able to use the database. Access to the server folder is approved by the System Administrator and controlled/maintained by Information Technology ITS through the Operations Support (OS) GetServices system."

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.

Information received in accordance with agreements/memoranda of understanding (MOUs) are covered in IRS Records Control Schedule (RCS) Document 12990 under RCS 8, item 52 (B1) which has a retention of 5 years after the processing year. Referrals with no further action taken are covered in Document 12990 under RCS 23, item 77 which has a retention of 3 years after the processing year.

SA&A OR ASCA

Has the system been through SA&A (Security Assessment and Authorization) or ASCA (Annual Security Control Assessment)?

No

Is the system secured in accordance with all applicable federal, treasury, and IRS security policy, procedures, and requirements?

Yes

Describe the system's audit trail.

Management must approve user access to the secure data transfer folders. Once approved, Information Technology (IT) will contact the folder point of contact for approval to grant permission the user permissions. The systems where the data is transferred and stored, once they leave the secure data transfer folders, require a Business Entitlement Access Request System (BEARS) request and managerial permissions prior to gaining access. These systems record audit trails. In the DOL SDT system, audit trailing is implemented. IRM 10.8.1 require auditing processes on each table and event. This auditing will include capturing the

following: insert date and time, inserted by, update date and time, and updated by; regarding each inbound/outbound file transfer request. The data that DOL-SDT receives is from the internal DOL systems which are deemed reliable, and the data is validated for accuracy by the DOL. DOL -SDT is following the appropriate audit trail elements pursuant to current Audit Logging Security Standards. The logs don't contain any PII or SBU data.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

System covers the initial process of receiving data before it is dispersed to the applicable function for investigation or other action.

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: Not Applicable

Contractors: Not Applicable

Members of the Public: Under 100,000

Other: Yes

Identify the category of records and the number of corresponding records (to the nearest 10,000).

10,000 pension and trust records

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