Date of Approval: **October 06, 2020**

PIA ID Number: **5353**

SYSTEM DESCRIPTION

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

Multi Employer Certification Application, MECA

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?

Multi Employer Certification Application, MECA, PIA # 2868

What is the approval date of the most recent PCLIA?

9/19/2017

Changes that occurred to require this update:

Expiring PCLIA

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.

TEGE Investment Executive Steering Committee 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 Employee Retirement Income Security Act (ERISA) §305(b)(3)(A) requires the Actuaries of multiemployer retirement plans to certify each plan year, to the Secretary of the Treasury and to the retirement plan sponsor whether or not the retirement plan is in endangered status. The Multi Employer Certification Application database (MECA) tracks and records the yearly Actuarial Certifications for multiemployers on funding status of retirement plans, as required by (ERISA) §305(b)(3)(A). It is estimated that between 1,300 and 1,500 plans are required to file Annual Actuarial Certifications for Multiemployer retirement plans.

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?

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

Phone Numbers

E-mail Address

Standard Employee Identifier (SEID)

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?

No

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.

Information entered into the MECA database is obtained from annual Multiemployer Certifications submitted by the retirement plan Actuary. EIN's are used for purposes of identification for that specific plan and contains relevant information needed from the certification to track funding progress. Contact information is needed to follow up if information is missing on the certification filed.

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

Data entry is performed by specific individuals. The information entered into the MECA database is obtained from annual Multiemployer Certifications submitted by the Plan Actuary. Validation rules are built into the database to ensure accuracy, timeliness and completeness of data.

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 50.222 Tax Exempt/Government Entities (TE/GE) Case Management 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?

No

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: Actuary Certification Letter
Transmission Method: Mail
ISA/MOU 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?

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?

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?

Notice is provided by ERISA §305(b)(3)(A), which requires the Actuaries of multiemployer plans to certify each plan year, to the Secretary of the Treasury and to the plan sponsor whether or not the plan is in endangered status.

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

No

Why not?

Annual certification via the ERISA law is not optional. Failure to comply could result in endangering the associated plan's status.

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

The MECA system has all the required multiemployer retirement plans preloaded in the database. As actuaries send in their certification letter, their database record is updated to reflect the date received and the status of the plan. These updates are conducted using drop down box and calendar options, to prevent entry errors. In the event the multiemployer plan is not in the database, it is manually added. The certification letter is saved per the Internal Revenue Manual. The MECA system is located on a secure shared 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 Modernization & Information Technology Services (MITS) through the OS GetServices system. Corrections made to the data are approved by the Project Manager and made by either the Project Manager or Tax Examiner.

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: Read Write

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

The MECA system is located on a secure shared 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 Modernization & Information Technology Services (MITS) through the 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.

All records housed in the MECA system will be erased or purged from the system in accordance with approved retention periods. It is the official repository for data and documents and has received National Archives approval to affect data disposition. Any records generated by the system will be managed according to requirements under Internal Revenue Manual 1.15.24 and will be destroyed using IRS Records Control Schedules 24, Item 53 and as coordinated with the IRS Records and Information Management Program and IRS Records Officer.

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.

The audit trail is maintained by MITS and access is granted through the OS GetService. MITS maintains records of individuals who have access to the shared server folder.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

This is an internally created Access database that did not follow an Information Technology (IT) path in development. The Business System Planning (BSP) office is investigating a potential enterprise solution.

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: Not Applicable

Other: Yes

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

Annual Actuarial Certification for Multiemployer Retirement Plans, 1500

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?

No