Date of Approval: **June 09, 2022**

PIA ID Number: **6997**

SYSTEM DESCRIPTION

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

Lockbox, Lockbox

Is this a new system?

Yes

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

The Web Apps Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Domain Architecture/Milestone 2

Preliminary Design/Milestone 3

Detailed Design/Milestone 4A

System Development/Milestone 4B

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 Lockbox Project will leverage the existing IRS Lockbox Network to digitize Form 940 that are mailed to the Lockbox sites and convert paper return documents to a digital format for electronic submission and processing in Modernized e-File (MeF). The Lockbox Project will result in a document intake solution that will increase data collection up front, optimize electronic file storage, and achieve full data capture for paper submissions.

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:

Another compelling reason for collecting the SSN

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

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
Protection Personal Identification Numbers (IP PIN)
Employment Information

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.

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.

Total Payments to all employees. Total of payments made to each employee in excess of $7,000.

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

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.

The taxpayer's information is required for each tax return. The information that is received from other internal IRS systems is used to validate the aforementioned information. The Transmitter and Electronic Return Originator (ERO) information received from the Transmitter and ERO is matched against the data collected from internal IRS systems.

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

After the paper forms are scanned in through the Lockbox sites, they are prepared as electronic returns and go through document perfection to be transitioned to the MeF-compliant format so that they can be electronically submitted. Each return prepared and

submitted to MeF for e-filing must adhere to the schemas and business rules. If a single data element fails the schema integrity check or business rule failure, the tax return is rejected. Electronic Tax Administration (ETA) supplies the business rules for each return type. MeF enforces the rules against the tax returns using a business rules engine. Business rules enforce relationships between data and forms. When MeF validates returns against the business rules, and if it encounters a discrepancy, the tax return is rejected. New schemas and business rules are issued for each new tax year. Any non-current returns (prior tax years) prepared and submitted must use that year's schema and business rule versions or the returns will fail the schema and business rule validation checks.

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 22.062 Electronic Filing Records

IRS 24.030 Customer Account Data Engine Individual Master File

IRS 34.037 Audit Trail and Security Records

IRS 24.046 Customer Account Data Engine Business Master File

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?

No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: 940
Form Name: Employer's Annual Federal Unemployment (FUTA) Tax Return

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: Modernized eFile
Current PCLIA: Yes
Approval Date: 2/8/2022
SA&A: Yes
ATO/IATO Date: 4/19/2021

Identify the authority.

E-Government Act of 2002, 5 USC 301 or 26 USC 6103(b)(1) and IRC 6103(n)

For what purpose?

Electronically submit official tax returns

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

No

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?

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?

The notice is provided on the respective form instructions.

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

No

Why not?

Information required to electronically file tax returns. Authority: Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations & PVR #15- Consent and #18- Individual Rights.

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

Due process is addressed by other IRS business departments that directly interact with taxpayers. Due Process is provided pursuant to Title 26 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).

Contractor Owned and Operated

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

IRS Employees

Users: Read Only

Managers: Read Only

System Administrators: Read Write

IRS Contractor Employees

Contractor System Administrators: Read Write

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

Internal Users (IRS Employees): Internal Users are subject to management, system administrator, data administrator, and security administrator approval via the Business Entitlement Access Request Service (BEARS). BEARS is used to document access requests, modifications, terminations for all types of users, including system administrators, system accounts requiring Electronic File Transfer Utility (EFTU) access, and test accounts. Contractors: Accenture users request access to the Integrated Enterprise Portal (IEP) environment through the Information Technology Security Management (ITSM) authorization process. To request a new account, changes to an existing account or removal of an account, the IRS Enterprise Portals Contractor Access Form is filled out. Upon completion of the form, an Accenture Program Management Office (PMO) resource will validate the request and create an access grant request within ITSM. ITSM will route the ticket to the appropriate task order lead to review and approve the requested level of access. Once approval is received, the ticket will be routed to the appropriate task order staff to create, edit, disable, or remove the account. Access will be approved in accordance with the principle of least privilege based on the intended system usage of the user. Administrators will only grant access permissions commensurate with the level authorized in the ITSM ticket. External Users: External users apply for access through e-Services. They must pass a suitability background investigation before being given access rights. When they pass the suitability background process, they are provided their Electronic Transmitter Identifying Number (ETIN) and Electronic Filer Identifying Number (EFIN). This process is external to MeF. For external third party and State Trading Partners who access Application to Application (A2A) or Internet Filing Application (IFA) through the Registered User Portal (RUP), account registration is performed through e-services and stored within Enterprise Directory and Authentication Services (EDAS). The application process mentioned above determines user's Role Based Access to MeF. As of MeF Release 10, A2A external trading partners are required to use certificate-based authentication. A2A users must enroll their systems using the E-Services Automated Enrollment application. The application uses the user's e-services profile to determine access rights. Transmitters are given transmitter access and roles but denied State agency roles. State agencies are given State agency access and roles but denied transmitter roles.

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.

RCS 19 Item 81-Modernized e-File (MeF) System. -(A) Inputs: The Modernized e-File System (MeF) end users register for IRS e- Services program and complete an application for

IRS e-file. After an applicant passes the suitability check and the IRS completes processing the application, the IRS notifies the applicant of acceptance to participate in IRS e-file. Transmitters and Software Developers must complete testing before final acceptance. The IRS assigns Electronic Identification Filing Numbers (EFINs) to all Providers and assigns Electronic Identification Transmission Numbers (ETINs) to Transmitters, Software Providers, and Online Providers. The following Form types are e-filed through the MeF platform as inputs: Corporations: Forms 1120, 1120-F, and 1120S. Exempt Organizations: Forms 1120-POL, 990, 990-EZ, 990-N (e-Postcard), and 990- PF. Partnerships: Forms 1065 and 1065-B. Excise Tax: Forms 2290, 720 and 8849 (Schedules 3, 5, 6 only) Extensions: Forms 7004 and 8868. MeF also supports a Fed/State program that consists of a single point of submission and retrieval for all registered transmitters and State agencies. This Fed/State initiative includes Corporations, Partnerships and Exempt Organizations. Additional MeF information can be found in Publications 4163 and 4164. AUTHORIZED DISPOSITION Delete/Destroy any cached transmission files 90 days after successful entry and verification into the MeF Repository. (B) System Data: System data in the Modernized e-File System (MeF) consists of the contents of all transmissions files from taxpayers. AUTHORIZED DISPOSITION Cut off at the end of each processing year. Delete/Destroy 75 years after cutoff. (C) Outputs: The Modernized e-File System (MeF) outputs support eFile and Modernized eFile Programs supported by the System (including Business Master File, Business Master File Returns Processing, End-User (public) documentation hosted on the IRS Internet web site. Documentation includes Internal Revenue Service Publications 3112, 3005, 1345, 1346, 1436, 1437, 1438, 1438-A, 1474, 3823, 4162, 4163, 4164, 4205, 4505, 4594, Revenue Procedure 2007-40 e-Glossary, Quick Alerts, and e-News. AUTHORIZED DISPOSITION Delete/Destroy when no longer needed for operational purposes. Note: MeF outputs are retained in the recipient electronic publications system as the official records. (D) System Documentation: System Documentation for the Modernized e-File System (MeF) consists of codebooks, records layout, User Guide, and other related materials. AUTHORIZED DISPOSITION Delete/Destroy when superseded or 5 years after the system is terminated, whichever is sooner.

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 system has been assessed under the Cyber Contractor Site Assessment process against the IRS Publication 4812 for Contractor Security Controls. The system audit trail is managed by automated log collection and analysis tools. Logs are written to the local system and then sent to the audit collection system for storage and review and analysis.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

Testing is conducted for troubleshooting purposes and on an ad-hoc basis. While a specific test plan does not exist, the Lockbox sites are following a defined testing process: associated with Security Technical Implementation Guides (STIGs) content published to the government checklist repository to determine compliance with system baseline requirements. These guides, when implemented, enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities. System Administrators (SA) are provided with validation instructions (Check Test) for the tested controls as well as corrective action steps ensuring remediation (Fix Text). Finding Details as well as Comments are added as evidence to the saved checklists by the SA To test and harden the system.

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: 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.

Not Applicable