

Date of Approval: **March 03, 2021**

PIA ID Number: **5935**

SYSTEM DESCRIPTION

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

Digital Mailroom, Digital Mailroom

Is this a new system?

Yes

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

Wage and Investment (W&I)

Current ELC (Enterprise Life Cycle) Milestones:

Preliminary Design/Milestone 3

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.

To provide immediate relief to Business campus employees from the growing backlog of paper submissions, Information Technology (IT) will establish a Digital Mailroom Minimum Viable Product (MVP) to reduce the amount of paper submissions that must be manually sorted for processing. The Digital Mailroom will allow the taxpayer to enter metadata and upload documents which would have been mailed in the past and make them available for the IRS processors to retrieve similar to how they retrieve the scans from the mailroom.

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

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

The Digital Mailroom will allow the taxpayer to enter metadata and upload documents which would have been mailed in the past and make them available for the IRS processors to retrieve similar to how they retrieve the scans from the mailroom.

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. This system 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.

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
Place of Birth
Mother's Maiden Name
Vehicle Identifiers
Passport Number
Financial Account Numbers
Photographic Identifiers
Employment Information
Tax Account 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:

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.

The taxpayer can include anything in a response such as:(pictures or responses to other issues). Cloud software will be utilized to ensure the taxpayer only provides responsive documents. Additionally, malicious code protections will be deployed to detect any malicious content.

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.

To provide immediate relief to Business campus employees from the growing backlog of paper submissions, Information Technology (IT) will establish a Digital Mailroom Minimum Viable Product (MVP) to reduce the amount of paper submissions that must be manually sorted for processing. The Digital Mailroom will allow the taxpayer to enter metadata and upload documents which would have been mailed in the past and make them available for the IRS processors to retrieve similar to how they retrieve the scans from the mailroom.

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

The PII maintained in the Digital Mailroom database is provided directly from existing IRS systems and approved programs. Accuracy and completeness of data is inherited from the existing IRS systems.

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 34.037 Audit Trail and Security Records

IRS 42.021 Compliance Programs and Projects Files

IRS 00.001 Correspondence Files and Correspondence Control Files

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: Taxpayer

Transmission Method: File upload

ISA/MOU: No

Does the system receive SBU/PII from Taxpayer forms?

Yes

Please identify the form number and name:

Form Number: Form 3219C
Form Name: Statutory Notice of Deficiency

Form Number: Form 4800C
Form Name: Questionable Credit 30 Day Contact Letter

Form Number: Form 1040
Form Name: U.S. Individual Income 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: IEP Integrated Enterprise Portal
Current PCLIA: Yes
Approval Date: 11/22/2019
SA&A: Yes
ATO/IATO Date: 4/16/2020

System Name: W&I RICS Automated Questionable Credits, AQC
Current PCLIA: Yes
Approval Date: 10/27/2020
SA&A: No

Identify the authority

5 U.S.C 301, 1302, 2951, 4118, 4308 and 4506 18 U.S.C. 1030 (a)(2)(B) 26 U.S.C. 7801
Executive Orders 9397 and 10561.

For what purpose?

To identify and track any unauthorized accesses to sensitive but classified information and potential breaches or unauthorized disclosures of such information.

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.?

Yes

Briefly explain how the system uses the referenced technology.

The taxpayer will visit the application link to upload the forms.

Does the system use cloud computing?

Yes

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

No

Please explain.

The Digital Mailroom application itself will be developed using the FedRAMP'd AWS GovCloud services. It will be incorporated into the EP FISMA Moderate security package.

Please identify the ownership of the CSP data.

IRS

Does the CSP allow auditing?

No

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?

Yes

Was an electronic risk assessment (e-RA) conducted on the system/application?

Not Applicable

Please explain.

For Phase 1, the taxpayer is not being authenticated into the system. This application is meant to mirror the existing mailroom process. Anyone can send mail to the mailroom without being authenticated.

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 and consent are provided in the tax forms and instructions pursuant to 5 USC.

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 in the tax forms and instructions pursuant to 5 USC. The IRS has the legal right to ask for information per Internal Revenue Code sections 6001, 6011, and 6012(a), and their regulations. The regulations state that "taxpayers must file a return or statement with IRS for any tax they are liable for".

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

The system will allow affected parties the opportunity to clarify or dispute negative information that could be used against them. Due process is 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 Contractor Operated

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

IRS Employees

Users: Read Only

Managers: Read Only

IRS Contractor Employees

Contractor Users: Read Write

Contractor Managers: Read Write

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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

All access request to the system will have to go through the formal Integrated Enterprise Portal (IEP) Systems Access Process. This request has to be approved by the potential user's manager based upon a user's position and need-to-know. If approved, the request is then forwarded to the administrators of the system for the creation of a new user identification and password.

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.

Automated Questionable Credits (AQC) records in the Digital Mailroom (Document Upload Tool) will be deleted or destroyed 21 days after verification of successful creation/download in accordance with GRS 5.2, item 020. Records will be managed according to requirements under IRM 1.15.1 and 1.15.6 and as coordinated with the IRS Records and Information Management (RIM) Program and IRS Records Officer. AQC records downloaded from Digital Mailroom (Document Upload Tool) will be managed in SharePoint according to requirements under IRM 1.15.1 and 1.15.6 and maintained for 7 years in line with individual tax returns under RCS 29, item 56.

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?

2/26/2021

Describe the system's audit trail.

The Digital Mailroom 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?

No

When is the test plan scheduled for completion?

2/26/2021

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 Security Assessment was conducted by the Cyber Cloud Assessment Team prior to Go-live. During this assessment, the applicable NIST controls were examined.

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: Under 5,000

Members of the Public: 100,000 to 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?

No