Date of Approval: **November 13, 2019**

PIA ID Number: **4568**

SYSTEM DESCRIPTION

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

Portal Account Replacement Tool, PART

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?

PART, PIA #4232

What is the approval date of the most recent PCLIA?

6/25/2019

Changes that occurred to require this update:

Addition of Personally Identifiable Information (PII)

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.

Enterprise Operations (EOps) Governance Board

Current ELC (Enterprise Life Cycle) Milestones:

Project Initiation/Milestone 1

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?

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 Portal Account Replacement Tool (PART) will support administrative account management functions for backend IRS user account directories that contain employee and taxpayer accounts. This tool replaces the employee and taxpayer account directory administration tools to improve security access controls and audit capabilities. The tool authenticates IRS directory administrators/users accounts, provides a user interface to manage the IRS hosted user account directories, and provide audit logs of their actions to the IRS audit repository. The tool receives user requests for IRS hosted user account directory data, displays the current state of user accounts, and allows the IRS directory administrators to manage user accounts. The Portal Account Replacement Tool resides within the IRS environment and allows employees to access the tool from the IRS Intranet using their credentials. The tool references unique account identifiers for employees and taxpayers. Information collected for the purpose of managing accounts will be encrypted and will require IRS users to also have access to the specific user account directory.

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?

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

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?

Yes

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

The Employee User Portal (EUP) pulls data from Corporate Authoritative Directory Service (CADS) for registration. CADS is utilized to verify that the employee is a legitimate employee. The following user information is required for registration purposes: Comprehensive employee identification information, IRS Universal Unique Identifier (UUID)and IRScustID for taxpayer identification. The tool mitigates the risk of using SSN by using alternative identifiers.

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)

PII for personnel administration is 5 USC

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.

PART will use the employee SBU/PII data in order to pass credentials through the existing Employee User Portal (EUP) Authentication process to validate user access to the solution. This will follow authentication at two levels and will be subsequent to the system administrators granting approvals through the first line manager or proxy, the application product owner, and the application administrator. Data relevant to the employee is only used for validation to the tool itself and the IRS directory administrators' SEIDs will be stored in the PART database to authenticate users to the endpoints they will be granted management access to. The tool stores references to the endpoint accounts using the naming attributes each IRS user account directory tree uses to enable the IRS directory administrators to browse and manage each endpoint. PART is internal to the IRS and will maintain no public information beyond the naming attributes. Data required for reporting of the user account directory endpoints will also be stored in the IRS environment within a secure reporting database on a separate reporting server. Strict access control policies are in place for this reporting server and audit logging is enabled.

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

Employee PII is obtained from the IRS Active Directory (AD). The accuracy of the information is based on obtaining employee data from the AD system, the manager of record and the employee themselves. Information is verified by the requester upon entering the application. Additionally, the employee must re-certify the information is correct before submitting the access request. Relevance of maintaining the information is verified by the application every 90 days by validating activity of the employee and taking the necessary steps to alert the employee of inactivity and removal of access between 90- and 120-day period if no longer required. Additionally, annual re-certification of access is required for all users. PART receives PII/SBU from the following backend directories (Enterprise Directory and Authentication Services (EDAS), Enterprise Application Integration Broker (EAIB), and eAuth 2.0), EUP SiteMinder, EDA, CADS, NTIN. Those backend directory endpoints validate the accuracy, timeliness, and completeness of the SBU/PII that they are providing.

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 36.003 General Personnel and Payroll Records

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: eServices
Current PCLIA: Yes
Approval Date: 4/20/2018
SA&A: Yes
ATO/IATO Date: 2/21/2018

System Name: eAuthentication
Current PCLIA: Yes
Approval Date: 7/10/2018
SA&A: Yes
ATO/IATO Date: 10/24/2017

System Name: Corporate Authoritative Directory Service (CADS)
Current PCLIA: Yes
Approval Date: 2/6/2017
SA&A: Yes
ATO/IATO Date: 6/14/2016

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?

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?

For the IRS employees, the individual must provide consent to the application in order for the data to be collected. This occurs during the OL5081 process. A second user rules-of-behavior must be agreed to before gaining access to the application. Consent must be provided for both as part of the validation and certification process. For taxpayers, notice is provided on the IRS.gov website. Notice, consent and due process are provided via the IRS systems and their related tax forms instructions, and pursuant to 5 USC.

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):

If the IRS employee chooses not to validate and certify during the request process, then the application exits, and the user is not allowed to continue with the request. Taxpayers can opt not to proceed with the online session. There is an alternate process available at the IRS to obtain the service the user is looking for. 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?

Information is provided by AD and verified by the user. Verification and consent are part of the certification process.

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 Only

Managers: Read Write

System Administrators: Administrator

Developers: Administrator

IRS Contractor Employees

Contractor Users: Read Only

Contractor Developers: Read Write

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

Access to the Computer Associates (CA) Identity Manager (IdM) is granted by having the appropriate approved OL5081 account approvals. Access approvals to this system is limited to the IRS Portal Account Management Section (PAMS). Additionally, access to SBU/PII data is on a need-to-know basis only and is determined by level of access granted. There are five user access levels that allow for different functionality to include: 1) Application Administrator: user who has the authority to configure, change and set up workflows, modify portal settings, remove users, view/take actions on incoming requests, and manage account inactivity; 2) Application Product Owner: reviews and approves or denies requests to specific applications based on action of first line manager; 3) Manager: reviews and approves or denies requests to any specific application per environment based on need to access to perform duties; 4) Manager Proxy: managers can name other employee to authorize user access in case they are not available; 5) Requester: user that needs access to any of the EUP-IEP applications listed in CA Identity Manager.

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.

The data in the CA Identity Manager tool application is backed up daily and weekly. Employee information is stored until the user no longer requires access to an application. Between 90 and 120 days of inactivity, the authorization is revoked, and the user information is deleted, except data maintained for audit history. Annual recertification follows the same process. Audit history information maintained can include initial application request and approvals; requests for changes to initial access and approvals; and revocation of access and approvals. The records are covered under General Records Schedule (GRS) 3.2: Information Systems Security Records. Records are eligible for destruction under GRS 3.2, item 6. Records are operational to establish or support authentication through AD. Included are policies and procedures; planning records; stand-up configuration and validation records; operation records; audit and monitor records; and termination, consolidation, or reorganizing records. Audit history information will be maintained per GRS 3.2, item 6 and will be hard deleted from the application and the disposal documented.

SA&A OR ASCA

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

In-process

When is the anticipated date of the SA&A or ACS completion?

3/5/2020

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 the PART SharePoint site.

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?

No PII is used in testing and all simulated data created is limited to the explicit purpose of testing the change request. Testers are limited to a few designated individuals and access to the development/test system is through the OL5081 process thereby providing for accountability and confidentiality of all testing functions and simulated data. All users complete Privacy Awareness training.

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: More than 100,000

Contractors: Under 5,000

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?

No