Date of Approval: **August 10, 2022**

PIA ID Number: **6892**

SYSTEM DESCRIPTION

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

Internal Identity & Access Management, IIAM

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?

Internal Identity & Access Management, IIAM, O&M

What is the approval date of the most recent PCLIA?

5/9/2019

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.

Security Services & Privacy Executive Steering Committee Advisory Board.

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.

Personal Identity Verification Data Synchronization (PDS) supports the Homeland Security Presidential Directive (HSPD-12) issued in 2004. HSPD-12 requires issuance of a common form of identity for all federal employees and contractors for physical and logical access, known as a Personal Identity Verification (PIV) Card, SMART ID, or SMART Card. This results in the integration of traditionally stove pipe operations for physical security, logical access, identity management and information technology. The purpose of these processes is to provide the right people with the right access at the right time. PDS is the implementation of processes, technologies, and policies to manage user identities throughout their lifecycle. The PDS digital identity lifecycle begins with identity being provisioned or created at the enterprise level in HR Connect (a human resource system that provides information to employees), then used when authentication, authorization, and access is required. Identity attributes are maintained, and updates can be made, e.g., job changes, name change, etc. At the end of the identity life cycle, the identity is deprovisioned, or removed from the systems upon separation of employment. The IRS PDS hub connects to Treasury HRConnect PDS via web services and synchronizes PIV related systems and identity data within the IRS. PDS allows required PIV and other critical HR information to be created from the authoritative sources (USAccess "(a program that Federal agencies utilize to issue approved credentials to their employees)", HRConnect) and allows for re-use of HR data to synch those data attributes with down level systems in near real time. A web service interface between the IRS PDS Hub and Treasury HR Connect PDS allows PIV data synchronization requirements to be met.

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:

Security Background Investigations

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

Federal agencies require in administration of their activities a system of accounts which identifies each person individually. The use of IRS employee's SSNs are permissible for personnel administration according to 5 USC & Executive Order 9397.

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. The Internal Identity & Access Management system requires the use of SSN's because no other identifier can be used to uniquely identify a federal employees or contractors.

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
Standard Employee Identifier (SEID)
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?

No

Cite the authority for collecting SBU/PII (including SSN if relevant).

SSN for personnel administration (IRS Employees) is 5 USC & Executive Order 9397

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.

When a new hire employee or contractor comes on board a digital identity is created after background checks and sponsorship have been completed. HR Connect will provide the new hire's name, Employee Identifier (EMPLID), and the Social Security Number (SSN) to the IRS identity systems to create the IRS Standard Employee Identifier (SEID), SEID is the unique identifier for IRS employees and contractors. Active Directory (AD) account, email address, date of birth and the User_principal_name (UPN) value which is required for the processing of the PIV card (smartID) in USAccess. This information (AD account (UPN value), email address and SEID will be provided back to HR Connect so it can be processed in USAccess to generate the PIV card.

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

With the PIV Data Synchronization (PDS) web service interface direct to HR Connect, we can better protect and streamline this process and eliminate multiple stops and multiple entry points for the identity data resulting in better accuracy of the data. When a new hire employee or contractor comes on board a digital identity is created after background checks and sponsorship have been completed. HR Connect will provide the Employee Identifier (EMPLID) and the Social Security Number (SSN) to the IRS identity systems to create the IRS Standard Employee Identifier (SEID), SEID is the unique identifier for IRS employees and contractors. Active Directory (AD) account, email address and the user_principal_name (UPN) value which is required for the processing of the PIV card (smartID) in USAccess. This information (AD account (UPN value), email address and SEID will be provided back to HR Connect so it can be processed in USAccess to generate the PIV card. Today for IRS this identity data synchronization process is managed by the Corporate Authoritative Directory Service (CADS) PDS services.

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.

Treasury .001 Treasury Payroll and Personnel System

GSA/Govt -7 HSPD-12 USAccess

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: HRConnect
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 10/27/2016

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)?

Yes

Please identify the form number and name:

Form Number: Form I-9
Form Name: Employee Eligibility Verification

Form Number: Form W-4
Form Name: Employee Withholding Allowance

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: HR Connect
Current PCLIA: No
SA&A: Yes
ATO/IATO Date: 10/27/2016

Identify the authority.

HR Personnel - personnel administration Title 5 USC.

For what purpose?

Hiring in HR Connect.

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?

We provide notice in accordance with the hiring notice requirements; Office of Management and Budget (OMB) M 03-22 & Privacy Requirements (PVR) #14- Privacy Notice and #19- Authorizations.

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

No

Why not?

HSPD-12 requires issuance of a common form of identity for all federal employees and contractors for physical and logical access, known as a Personal Identity Verification (PIV) Card, SMART ID, or SMART Card. This is a condition of employment.

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

Employee rights are covered through appropriate legal and National Treasury Employees Union (NTEU) contractually negotiated process for remediation.

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

Managers: Read Write

System Administrators: Read Write

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

Based on need to perform job duties during the hiring and badging processes and the requirements for performing system administration on the system. Access to the data is strictly controlled for administrators and HR specialists through Business Entitlement Access Request System (BEARS) approvals and is limited to those with an operational need to

access the information: Credentialing specialists and sponsors Network Administrators with operational responsibilities System Administrators with operational responsibilities Desktop Support Helpdesk Only items relative to the context of the user or administrator should be displayed. (e.g., administrative feature that would otherwise not be configurable by the user should not be displayed to the user.)

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.

Records are maintained in accordance with General Records Schedules 5.6, item 120, published in GRS Document 12829. However, many of the modules retain data indefinitely until purged from the system. When necessary, the system administrators request that the oldest data in the system is backed up and then dumped from the system. This is not an automatic process but must be requested.

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?

6/8/2021

Describe the system's audit trail.

Audit trails will be maintained, and reviews performed to identify unauthorized access in accordance with IRM 10.8.1.3.3 Audit and Accountability Policy and Procedures.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

IIAM project is now operational. There is no longer a need for a System test plan.

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: More than 10,000

Members of the Public: Not Applicable

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