Date of Approval: **April 26, 2023**

PIA ID Number: **7674**

SYSTEM DESCRIPTION

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

RPA User and Network Services Local Area Network, UNS LAN Unlock

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?

UNS Process Automation, UNS Auto, # 4881

What is the approval date of the most recent PCLIA?

4/3/2020

Changes that occurred to require this update:

Significant System Management Changes

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.

Enterprise Services Governance Board (ESGB)

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?

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 most frequent use case for the User and Network Services (UNS) Service Desk Call Center is when a customer (an IRS employee or contractor) becomes locked out of their Local Area Network (LAN) or Windows environment. This is most often due to entering their password incorrectly three times. The call is routed to a UNS Service Desk Specialist who opens a ticket, verifies the account is active, and performs the unlock. LAN unlock issues result in the highest number of call volumes for UNS. The number of calls often spikes after the customer returns from vacation or after major disruptions, for example, a government shutdown. By automating several parts of this process, the average call time would significantly decrease and allow the Service Desk Specialists to process more LAN unlocks or focus on troubleshooting more difficult issues that require human interactions. The automation will prompt the specialist to enter the caller SEID, open a ServiceNow ticket, unlock the account in Applications Development (AD) if the account is not active and locked, prompt the specialist to check if the caller can log in. The automation will close the ServiceNow ticket if the unlock is successful, or if the account is inactive, then search for additional open ServiceNow tickets for this caller for the specialist to review upon closure of the LAN unlock.

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.)?

No

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
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 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.

Automation will be programmed to access only what is relevant to complete the manual process. Automation will access enterprise systems such as ServiceNow, BEARS and Qwert to unlock employee/contract LAN access. These processes will require the use of sensitive information such as SEID to meet the requirements of the automated process.

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

Audit log files will be generated by the process automation and limited scale operational business reports will be provided.

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

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: ServiceNow
Current PCLIA: No
SA&A: No

System Name: BEARS
Current PCLIA: No
SA&A: 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?

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.?

Yes

Briefly explain how the system uses the referenced technology.

LAN Unlock - Given a caller SEID inputted by a specialist, this automation will accomplish: * The bot will prompt the specialist to enter the caller SEID * The bot will open a ServiceNow ticket * The bot will verify the caller account is active via BEARS (Business Entitlement Access Request System) * The bot will unlock the account in AD if the account is active and locked * The bot will prompt the specialist to check if the caller can log in * The bot will close the ServiceNow ticket if the unlock is successful, or if the account is inactive * The bot will search for additional open ServiceNow tickets for this caller for the specialist to review upon closure of the LAN unlock. No further action by the bot.

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?

No

Why not? If information is not collected directly from an individual, please discuss the factors considered in deciding to collect information from third party sources.

Process does not require collecting information from the individual. Any required information is collected from existing IRS systems.

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

No

Why not?

Process does not require collecting information from the individual. Any required information is collected from existing IRS systems.

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

Process follows â€˜KM00055506- BEARS - VERIFYING IDENTITY / USER PROOF FUNCTION' to verify user's identity.

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: Administrator

System Administrators: Administrator

Developers: Administrator

IRS Contractor Employees

Contractor Users: Administrator

Contractor System Administrators: Administrator

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

Existing approved help desk specialist will run the automation on their laptop, with their prior approval to access PII and SBU data if necessary.

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.

Other than log files, no other data is stored. The log file retention period will be determined by the source systems policies and procedures. GRS 3.1 Item 010-Infrastructure project records-Destroy 5 years after project is terminated, but longer retention is authorized if required for business use. GRS 3.1, item 020- Information technology operations and maintenance records. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

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?

5/31/2023

Describe the system's audit trail.

Security checks are in place to verify and track records of activities. Security packages and related Control Impact Assessment (CIA) requests were submitted to Security Assessment Services (SAS) to verify any changes made to the system and establish a security audit trail for the system.

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)?

Test results are stored on the RPA 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?

Test plans are generated and reviewed by process SMEs to verify and sign off that the automation only performs the same activities as the current manual process.

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: 50,000 to 100,000

Contractors: Under 5,000

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