Date of Approval: **December 10, 2020**

PIA ID Number: **5565**

SYSTEM DESCRIPTION

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

KNOWLEDGE INCIDENT/PROBLEM SERVICE AND ASSET MANAGEMENT, KISAM

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?

Knowledge, Incident/Problem Service and Asset Management, KISAM, PIAMS #2952

What is the approval date of the most recent PCLIA?

10/18/2017

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.

ENTERPRISE OPERATIONS (EOps) GOVERNANCE 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?

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.

KISAM operates on both the Windows 2012 and Redhat 6 operating systems. It is composed of various Commercial Off The Shelf (COTS) software packages, including Hewlett Packard (HP) Asset Manager, HP Service Manager, Oracle 12c database, Internet Information Services (IIS), HP Connect Information Technology (IT), and the Universal Configuration Management Database (UCMDB). HPAsset Manager manages the inventory of IT hardware and software assets and non-IT Assets. HP Service Manager is a tool used by help desk personnel, service providers and customers for submitting and managing user requests and incident/problems, for managing changes, providing a knowledge base, a service catalog and other submodules of HP Service Manager that may be needed to provide Information Technology Infrastructure Library (ITIL) based services.

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

Mailing address

Phone Numbers

E-mail Address

Standard Employee Identifier (SEID)

Employment Information

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.

The need to collect information on employees, to authenticate the customer and to validate are who they say they are.

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

The PII information is downloaded from the Corporate Authoritative Directory Service (CADS) every night.

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: Graphic Database Interface (GDI)
Current PCLIA: Yes
Approval Date: 4/26/2020
SA&A: Yes
ATO/IATO Date: 10/10/2019

System Name: HR Connect (HRCON)
Current PCLIA: No
SA&A: No

System Name: Password Management (PWM)
Current PCLIA: Yes
Approval Date: 3/29/2018
SA&A: Yes
ATO/IATO Date: 8/18/2018

System Name: HPE Universal Configuration Management Database (ECMS/UCMDB)
Current PCLIA: No
SA&A: No

System Name: Warehouse & Transportation Management System (WTMS)
Current PCLIA: No
SA&A: No

System Name: Corporate Authoritative Directory Services (CADS)
Current PCLIA: Yes
Approval Date: 12/4/2019
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?

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: Business Performance Management System (BPMS)
Current PCLIA: Yes
Approval Date: 10/7/2019
SA&A: Yes
ATO/IATO Date: 10/28/2020

System Name: Graphic Database Interface (GDI)
Current PCLIA: Yes
Approval Date: 4/26/2020
SA&A: Yes
ATO/IATO Date: 10/10/2019

System Name: HPE Universal Configuration Management Database (ECMS/UCMDB)
Current PCLIA: No
SA&A: No

System Name: Warehouse & Transportation Management System (WTMS)
Current PCLIA: No
SA&A: No

System Name: Employee Connection Reporting Services (ECRS)
Current PCLIA: Yes
Approval Date: 9/4/2020
SA&A: Yes
ATO/IATO Date: 10/16/2020

Identify the authority.

Internal Revenue Code sections 6001, 6011, and 6012

For what purpose?

Tax administration

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?

Notice, consent and due process are provided via an introductory screen at the start of KISAM access, 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):

The system will allow affective parties the opportunity to clarify or dispute negative information that could be used against them. Notice, consent and due process are provided pursuant to 5 USC.

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

It is determined by the OL5081 process. Employee requests, manager approves, the Point of Contact (POC) for that business unit approves, then the Systems Administrator (SA)'s for KISAM process the OL5081 request. Notice, consent and due process are 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 Operated

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

IRS Employees

Users: Read Only

Managers: Read Write

System Administrators: Read Write

Developers: Read Write

IRS Contractor Employees

Contractor Users: Read Only

Contractor Managers: Read Write

Contractor System Administrators: Administrator

Contractor Developers: Read Write

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

It is determined by the OL5081 process. Employee requests, manager approves, the POC for that business unit approves, then the SA's for KISAM process the OL5081 request. 1. A potential user will request access via the OL5081 application. This request has to be approved by the potential user's manager based on a user's position and need-to-know.

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.

HP Asset Manager data is approved for destruction 3 years after equipment disposal. Service Center data is approved for destruction 3 years after date of problem resolution. The End User Equipment and Services (EUES) Policy, Coordination and Asset Management (PCAM) group has ownership, responsibility, and accountability for the data described above. KISAM records can also be referenced under GRS 3.1, Item 020; also 3 year scheduled retention.

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?

5/26/2020

Describe the system's audit trail.

Use of the data/information in KISAM is captured in several ways: 1. In Service Manager, all records have sysmoduser and sysmodtime fields which record when and by whom records were modified. This applies to ticket data as well as system objects. 2. In Service Manager, there are activity records that record who/what/when for certain ticket updates. 3. In Service Manager, application log files record user log on/off, long running queries and any run time errors encountered. 4. In Asset Manager, events and changes to over 300 data elements in 30+ tables are recorded in a history table. Prior/New values and the user making the change are stored in this table. 5. In Asset Manager, a comments field is updated when changes are made by administrators, Asset Management Program Office users, the Barcode Scanner integration or the Inventory integration.

PRIVACY TESTING

Does the system require a System Test Plan?

No

Please explain why:

IRM 10.8.2, Security, Privacy & Assurance, Information Technology Security.

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