United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Agency Asset Management System (AAMS)	
Preparer: James Cunningham, Jackie Brown	**Office:** Office of Mission Support (OMS), Office of Administration (OA) / Attain LLC.
Date: 04/01/2020	**Phone:** (202) 564-7212/ (202) 564- 0313/ (443) 889-7402
Reason for Submittal: New PIA____ Revised PIA____ Annual Review __X__ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐	

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

The Agency Asset Management System (AAMS) provides EPA with enterprise-wide asset management for tracking physical and financial accountability for all EPA assets. As specified in the EPA Personal Property Manual 4832, dated June 2017, personal property is defined as any property, except real property. Personal property is analogous with using the word ‘asset’, both of which are generally used to define an item that is a ‘physical’ object. An asset is ‘accountable’ when it meets the threshold value of $5,000 or more. Any asset that is ‘non-accountable’ is below the $5,000 threshold. However, property that is categorized as sensitive, pilferable or controlled must be maintained as accountable property regardless of cost.

The AAMS is the sole system authority for all Agency physical assets.

The primary objectives for managing the EPA personal property portfolio are to:

- Establish effective planning and scheduling of requirements to ensure that sufficient personal property is available to support the strategic needs of EPA operations.
- Maximize the utilization of personal property and its return on investment.
- Ensure that property is used for official purposes.
- Effectively manage the inventory by providing for proper storage, maintenance, preservation and accountability of property.

The data collected in AAMS is used; a) for reporting annual wall-to-wall physical inventories of all accountable assets; b) assignment of assets to employees via a property decal; c) financial reporting of capitalized Agency assets; d) management of non-accountable personal property; and e) recording of asset lifecycle transactions from acquisition through disposal.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

The statutory authority for the Agency Asset Management System can be found in

- 44 U.S.C. § 3506, which establishes federal agencies' responsibilities for managing information resources and 40 U.S.C. § 11315, which establishes the responsibilities of the agency's Chief Information Officer to manage agency information resources.
- The Title III of the E-Government Act of 2002 - Federal Information Security Management Act (FISMA) – Public Law 107-347
- Federal Management Regulation: 48 CFR §1545, Government Property; 48 CFR §52.245, Government Property; and 48 CFR Chapter 15, EPA Acquisition Regulations.
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Special Publication (SP) 800-18 Revision 1, Guide for Developing

Security Plans for Federal Information Systems
- NIST Special Publication (SP) 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems
- The Federal Property and Administrative Services Act of 1949, as amended
- The Federal Property Management Regulations (FPMR), Title 41, CFR Chapter 101 and 102
- Department of Justice Property Management Regulations and Bulletins
- The Chief Financial Officers Act of 1990

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes, a System Security Plan (SSP) has be developed. The system currently has an ATO that will expire on 2 AUG 2021.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No ICR required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRamp approved? What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

No, the data will not be stored in the cloud.

Section 2.0 Characterization of the Information

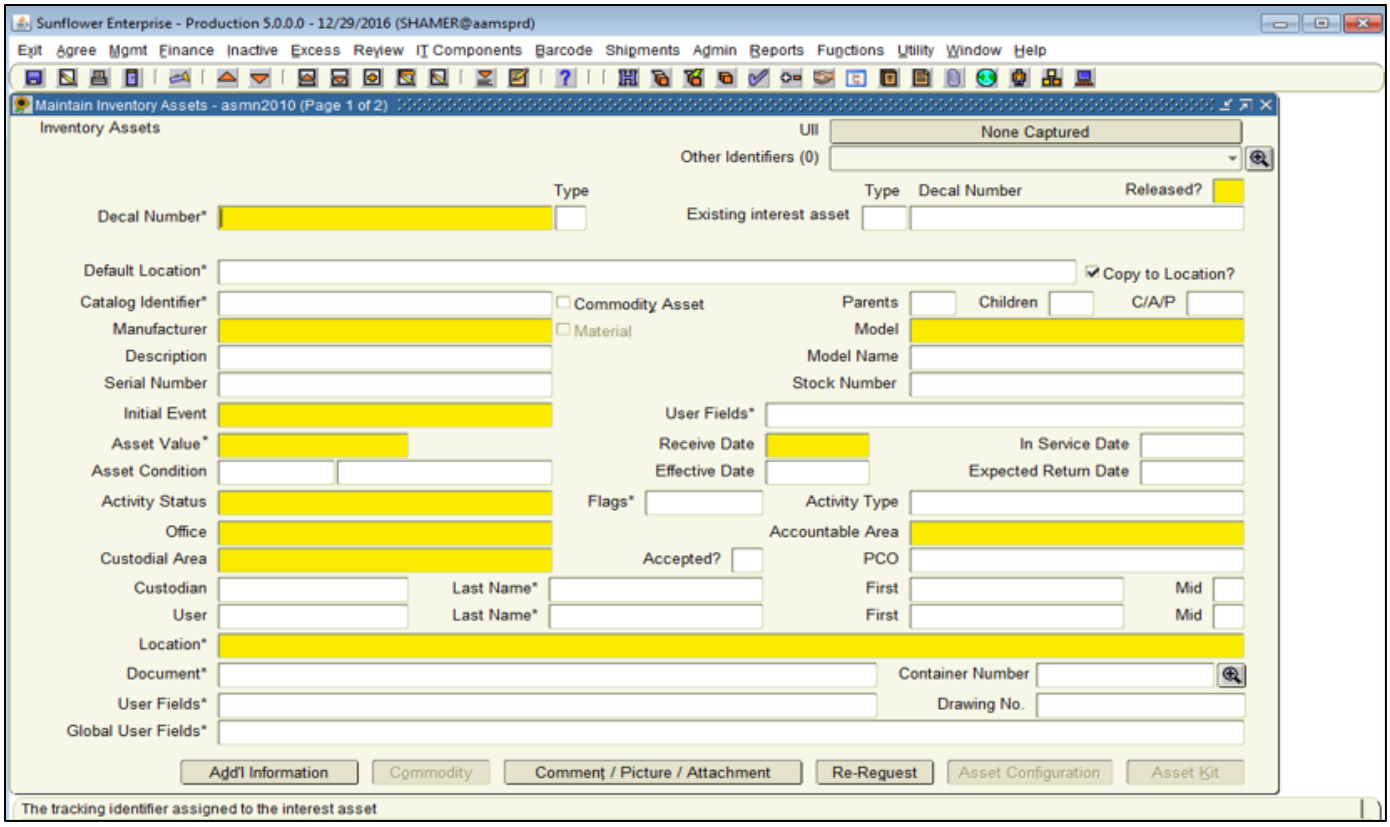
2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

There are two sources of information in the system:

A. Any employee with asset management responsibilities (federal or contractor employee) will manually enter information about assets within their area of responsibility. Personally, Identifiable Information (PII) includes:

- Custodian Name (First and Last and middle initial)
- User Name (person to whom the asset is assigned) (First and last and middle initial)

Figure 1, Sample Image of the Assets' Record below is an example of asset data captured in AAMS to manage EPA's accountable assets:



B. The Office of Administration has established a one-way communication database link from the Office of Administration Services Information System (OASIS) database. The link allows for automatically filling in attributes of the employee when EPA Federal and Contractor personnel on-board or off-board. This helps to avoid typos when manually entering the information, it ensures proper names are used, avoids conflicts when employees share the same first, middle or last names, also it streamlines the process for the assignment of personal property, while alternatively prevents the assignment of personal property to people that separate from the EPA. The database link automatically uploads the new employee attribute into a database table which is accessible only by authorized system administrators with elevated privileges and includes the following data elements:

- Workforce ID
- First Name
- Last Name
- Middle Initial
- EPA Email Address
- Phone Number
- Location (City, State)

During the asset data entry process, the Property Manager (system end user) assigns the asset to an employee or contractor by selecting a subset of the information from OASIS via a validated list of values to prevent manual data entry. This modified data view includes the Workforce ID, First Name, Last Name, and Middle Initial.

2.2 What are the sources of the information and how is the information collected for the system?

In addition to the utilization of EPA personal property, as authorized and documented throughout the property management lifecycle, the source of information for AAMS is the asset as it is acquired via purchase order or purchase card. When an asset arrives to an EPA warehouse, it is decaled and entered into the AAMS system, beginning the property management lifecycle. A "property management lifecycle" is a framework, much like NIST outlines a "framework for risk management". The lifecycle is determined by law and regulation. https://www.gsa.gov/policy-regulations/regulations/federal-management-regulation-fmr?asset=102167 **.** The property record shall be updated in the Agency Asset Management System (AAMS) when there is any change in authorized user, movement or transfer of property from one program/region to another, when property is loaned or borrowed, sold, or any other activity that changes title, accountability or stewardship. Using the image above, if an Asset Manager needs to change the location of an asset, it is simply manually entered into the location field.

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No

2.4 Discuss how accuracy of the data is ensured.

AAMS contains both structured and unstructured data, although unstructured data is limited to prevent data quality issues. An audit trail history of any change to the asset's record can be found in the asset's summary and history timeline. The audit trail history cannot be manipulated. Persons added to AAMS that are associated with an asset is obtained via a database link to OASIS to ensure accuracy.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

The AAMS contains PII but not sensitive PII.

Mitigation:

Mitigation for PII data contained in AAMS is by role-based access to the AAMS system. As it pertains to managing the Agency's assets, the asset's record requires the minimal amount of PII. The PII allows for full accountability throughout the lifecycle of the asset (when it arrives on the warehouse to its disposal from the agency). AAMS also uses role-based access control where only authorized personnel are allowed access using the "principles of least privilege"

Section 3.0 Access and Data Retention by the system

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes, system end user access control levels are within the system to prevent authorized users from accessing information they don't have a need to know. User based permissions restrict the information that may be viewed or modified. As system end users are assigned, they are given permission that is commensurate to their property responsibilities and is consistent with assigned job responsibilities necessary for the user to carry out assigned job functions. Privileges granted for that purpose must comply with the principles of least privilege, which requires that each user be granted the most restrictive set of privileges needed for the specific task.

3.2 What procedures are in place to determine which users may access the information and how does the system determine who has access?

AAMS roles are identified in the AAMS Property Policy and Procedures manual. Users assigned to the roles are provided access AAMS, at the appropriate level. For authentication purposes, AAMS utilizes the Agency Active Directory. Only users that have been granted the appropriate privileges will be allowed access to AAMS.

An approval workflow has been established to ensure authorized access is granted in accordance with the role. Any employee assigned a property role will need to submit an end user system access request to the sponsor of the AAMS using the following AAMS System Access Request. The AAMS supports OA's Real Property Services Division (RPSD), who is the sponsor. The OA's Resources Management Staff IT support group manages the AAMS on behalf of the RPSD. The RMS-IT Group does not approve/deny requests for systems access.

Following are the roles granted to AAMS users. The use of role-based access implements the principle of least privilege:

- Property Management Officer
- Property Utilization Officer
- Property Accountable Officer
- Property Accountable Representative
- Property Custodial Officer

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

The AAMS Application utilizes the Agency Active Directory for authentication purposes. Only users that have been granted the appropriate privileges will be allowed access to AAMS. Contractors with system user access have appropriate FAR clauses included in their respective contracts. The following FAR clauses will be included in the contract:

- 52.224-1
- 52.224-2
- 52.224-3

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

The OA's Real Property Services Division with oversight of the Property Management Program, has an approved Agency Records Schedule 0089, Administrative Support Databases. NARA regulations require that electronic records be retrievable and usable for as long as needed to conduct Agency business and meet NARA-approved disposition. The electronic software program is covered by schedule 1012, item e Data within AAMS is closed when superseded, updated, replaced or no longer needed for current agency business.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

The nature of privacy data contained in AAMS is very low risk. Data may be retained longer than needed. AAMS comply with EPA records schedule 0089. This schedule uses NARA Disposal Authority: DAA-GRS-2013-0002-0016 thus asset records are retained up until the data is closed when superseded, updated, replaced or no longer needed for current agency business. Generally, this occurs when the physical asset is disposed, meaning sold to GSA for resale. The Federal Management Regulation, CFR Parts 102-36 through 102-42 defines the disposal categories for all assets. Asset records identified as "Remaining Active" in AAMS means the assets' record can continue to be retrieved in the AAMS. The risk is the presence of AAMS information and its unauthorized exposure. When records are removed from AAMS, so are the associated risks.

Refer to Figure 1: Sample Image of the Assets' Record

Mitigation:

AAMS comply with EPA records schedule 0089. This schedule uses NARA Disposal Authority: DAA-GRS-2013-0002-0016 thus asset records are retained up until the data is closed when superseded, updated, replaced or no longer needed for current agency business. Periodic reports mitigate the privacy risk associated with asset records in AAMS that exceed EPA records schedule 0089 mandate. In addition, reports are run to ensure persons no longer with the agency do not retain assets in AAMS. Until the asset has been disposed in accordance with the FMR, the asset's electronic record will remain "active" in AAMS. Once officially sold by GSA, the asset record will be "closed", after which the asset record is destroyed 3 years after file closure. Once the record is removed from AAMS, the risk is removed.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

No. AAMS information is not shared outside of EPA as part of the normal agency operations. None.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

None.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

None.

4.4 Does the agreement place limitations on re-dissemination?

None

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

None.

Mitigation:

None.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

5.1 How does the system ensure that the information is used in accordance with stated practices in this PIA (Section 6.1)?

Every transaction involving EPA accountable property shall be recorded in the official property record in the Agency Asset Management System (AAMS). Recording property transactions and events is the responsibility of the designated Asset Managers. All asset records in AAMS are deemed the official records and shall serve as the official property record.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

The EPA's Information Security Program provides annual security and privacy training to all employees. Only authorized system end users have access to the system. All system end users must adhere to federal and Agency directives related to privacy policies and procedures.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is a low risk of improper audit leading to unaccounted data.

Mitigation:

Windows server and database auditing frequency and proper auditing is in place, operating as expected and generating the desired results.

The SPLUNK tool is used to capture operating system and database audit logs and format reports for human consumption

The EPA PPM 4832 identifies the minimum property record data elements, as revised, to establish an official property record in the AAMS. Program/regional offices with specific new data element requirements shall contact the APMO for review and designation as an official EPA property record data element in the AAMS. A copy of the manual can be found at: http://intranet.epa.gov/ohr/rmpolicy/ads/manuals/4832-EPA-Personal-Property-Policy-and-Procedures-Manual-8-15-2017.pdf

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

The data collected in AAMS is used; a) for reporting annual wall-to-wall physical inventories of all accountable assets; b) assignment of assets to employees via a property decal; c) financial reporting of capitalized Agency assets; d) management of non-accountable personal property; and e) recording of asset lifecycle transactions from acquisition through disposal.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X__ No __. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

The system is designed to retrieve information as identified in section 2.1 to include to the following data elements:

- Workforce ID
- First Name
- Last Name
- Middle Initial
- EPA Email Address
- Phone Number
- Location (City, State)

6.3 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Privacy Act System of Records: Office of Administrative Services Information System (OASIS), EPA-41. Identifiers used by AAMS are retrieved from EPA-41 via data base links.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Risks related to use of information are that personnel granted access to AAMS may use information in ways not intended.

Mitigation:

The SPLUNK tool is used to capture OA and database audit records. These audit records include read, update, addition and delete transactions. This capture is done in near real time and historical information is kept for up to one year or longer. Only authorized users of the AAMS will be provisioned for end user system access. Role-based security is established using the principle of least privilege. Protecting PII in AAMS is therefore carefully conducted based upon the privacy engineering framework of: predictability, manageability and dis-associability.

Predictability: An approval workflow has been established to ensure authorized access is granted in accordance with the role. Any employee assigned a property role will need to submit an end user system access request to the sponsor of the AAMS.

Manageability: End user access is provisioned based upon the approved role.

Dis-associability; Once granted, only authorized system end-users can view asset records in their specific organizational unit as they pertain to their asset management role. For example, a Custodial Officer's system access role will not have the same view into the asset inventory as a Property Management Officer system access role within the same organizational unit. Alternatively, Custodial Officer in an organization unit located in RTP cannot view the same asset records for Custodial Officer's located in another organization unit, like Region 9 San Francisco.

Accountability: All account access security controls are implemented in accordance with NIST 800-53 and documented in the SSP.

*If no SORN is required, STOP HERE.

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

AAMS privacy related information is collected during the on-boarding process for federal or non-federal employees. Any individual who wants to know whether this system of records contains a record about him or her, who wants access to his or her record, or who wants to contest the contents of a record, should make a written request to the EPA FOIA Office, Attn: Privacy Act Officer, MC2822T, 1200 Pennsylvania Avenue, NW., Washington, DC 20460.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

During the on-boarding process, opportunities are available for individuals to consent to use or decline to provide information. As a condition of employment individuals are required to provide information requested and agree that the information provided may be shared for EPA business purposes.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Not giving adequate notice to individuals.

Mitigation:

Adequate notice is given to individuals.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their

information?

Employees who wishes to obtain their information about agency assets shall contact their local Agency Records Officer liaison.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

An individual who wishes to make corrections to the assets' record can do so by contacting their local Agency Records officer liaison. A data element is an individual piece of descriptive information collected about an asset to populate the property record in the AAMS. Any changes, or corrections, to the data elements associated with assets' record can be made in the system. All personal property transactions recorded in the AAMS must be have a documented audit trail. Only authorized system end users can make corrections to the assets record.

8.3 How does the system notify individuals about the procedures for correcting their information?

The system does not notify individuals about correcting their PII information. Individuals can send notification for correcting asset information to the OA RPSD program office, David Shelby, National Agency Property Manager.

8.4 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

There is proper procedure in place for redress.

Mitigation:

None