PRIVACY IMPACT ASSESSMENT

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

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx

System Name: Office of Administration Services Information System (OASIS)	
Preparer: Jackie Brown **System Owner: James Cunningham**	**Office: Office of Mission Support (OMS) Enterprise Administrative Systems Division (EASD)**
Date: August 8, 2024	**Phone: (202) 564-0313**
Reason for Submittal: New PIA____ Revised PIA__X__ Annual Review____ 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:

Office of Administration Services Information System (OASIS) an internet-based portal that provides uniform data storage and access for several business processes within Office of Mission Support (OMS) Enterprise Administrative Systems Division (EASD). These business processes consist of multiple software "modules" each of which represents a distinct business function and dataset.

The PIA is being revised to incorporate changes to OASIS including but not limited to hosting platform changes, the addition of new modules and the removal of modules that no longer provide business value. Below is a list of modules and their business process descriptions.

Count	Title	Business Process
1	**Credential Badging**	Generate and manage issuance and expiration of Credential badges used to access restricted EPA labs
2	**Driver Tracking**	Manage headquarters (HQ)-EPA's executive motor pool fleet of vehicles and track and report on EPA Vehicle usage trends.
2	**Environmental, Health and Safety**	Track and report environmental, health and safety regulatory compliance
4	**EPA Automotive Statistical Tool (AST)**	EPA's fleet management information system, which houses life-cycle fleet data such as acquisition costs, vehicle identification, operating costs, fuel consumption, and disposal proceeds.
5	**HQ Project Management**	Provide Facilities Management and Services Division (FMSD) with the capability to manage HQ facility projects.
6	**Incident Reporting**	Physical security incidents reporting system for headquarters. Office of Real Property, Safety and Security /Security Management Division (SMD).
7	**Mail Center**	Record and track postal transaction costs associated with the Agency's incoming and outgoing mail and reconcile the costs with Office of the Chief Financial Officer (OCFO) Compass financial system
8	**National Security Information**	Supports SMD's responsibility for implementing the agency's national security information program.
9	**Parking System**	Record, manage, allocate HQ parking spaces.
10	**Print Request Form**	Provide HQ employees the capability to submit document print requests.
11	**Print Request Tracking**	Track and maintain information regarding Print Job Orders for Headquarters Print Shop and manage Print Shop costs associated with these orders.
12	**Personal Security System (PSS)1 Archive**	Provide SMD Physical Security Branch (PSB) the capability to read legacy PSS1 data.

13	**Transit Management**	Provide FMSD with the capability to manage HQ employees Transit Subsidy accounts.
14	**Transit Subsidy Program Enrollment**	Provide HQ employees the capability to register and update their Transit Subsidy accounts.
15	**USA Performance**	Using data from EPA's Federal Personnel and Payroll System (FPPS) OASIS is used as a pass-through feature to the Office of Personnel Management's (OPM) USA Performance (USAP) System. USAP is an OPM software solution to assist Federal agencies, including EPA, in implementing their Senior Executive Service (SES) and Non-SES performance management program and systems. USAP is owned and operated by OPM as a Federal Shared Service. The performance records contained in USAP are covered by the OPM/GOVT-2 Employee Performance File System Records System of Records Notice (SORN).
16	**User Management**	The purpose of this application is to provide the user with the required roles for the applications contained in OASIS.
17	**Lab Management**	Manage EPA Lab and Chemical Inventory

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?

- 5 U.S.C. 301; Federal Information Security Act (Pub. L. 104-106, sec. 5113)
- Electronic Government Act (Pub. L. 104-347, sec. 203); the Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504)
- Federal Property and Administrative Act of 1949, as amended.
- Title 44 USC section 501.
- Executive Order 12968 - Access to Classified Information
- Executive Order 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information
- Code of Federal Regulations, Title 5, Part 732 - National Security Positions
- Code of Federal Regulations, Title 32, Part 2001 - Classified National Security

Information

- Executive Order 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust
- Executive Order 13526 - Classified National Security Information
- Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
- Executive Order 13764 - Amending the Civil Service Rules of EO 13488 and EO 13467
- Intelligence Community Directives
- Security Executive Agency Directives (SEADs);
- Office of Personnel Management's (OPM's) Suitability Handbook
- OPM Federal Investigations Notices (FINs)
- Government Organization and Employees (5 U.S.C. 301)
- Public Buildings under the control of Administrator of General Services (40 U.S.C. 3101)
- Federal Information Security Management Act of 2002 (44 U.S.C. 3541)
- Executive Order 9347 (Nov. 22, 1943)
- Security Executive Agent Directive 3 (SEAD 3), 12June2017
- Sections 1104, 3321, 4305, and 5405 of title 5, U.S. Code, and Executive Order 12107

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 has been completed for this application. The OASIS ATO expires on October 13, 2025.

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 Information Collection Request (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. PII data will not be stored in the cloud.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

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

Count	Title	Data Elements
1	**Credential Badging**	First Name, Last Name, Work Force Identification (ID), Work Email Address, and Credential Number
2	**Driver Tracking**	First Name, Last Name, Work Email, and Work Phone Number
2	**Environmental, Health and Safety**	First Name, Last Name, Work Email Address, Social Security Number (SSN), and Blood Type
4	**EPA Automotive Statistical Tool (AST)**	First Name, Last Name, Work Phone Number, Work Email, Work Phone, SSN, Home Address, Date of Birth (DOB), and Work Address
5	**HQ Project Management**	First name, Last Name, Work Email Address, and Work Phone Number
6	**Incident Reporting**	Local Area Network (LAN) ID, First Name, Last Name, and Work Telephone
7	**Mail Center**	First Name, Last Name, and Work Email,
8	**National Security Information**	First Name, Last Name, Middle Initial, SSN, Work Force ID, Personnel ID, City, State, and Zip Code
9	**Parking System**	First Name, Last Name, Middle Initial, Workforce Id, Permit Number, Address, and Work Email
10	**Print Request Form**	First Name, Last Name, Work Email Address, and Work Phone Number
11	**Print Request Tracking**	First Name, Last Name, Work Email Address, and Work Phone Number

12	**PSS1 Archive**	First Name, Last Name, Middle Initial, Workforce Id, Personnel ID, Case Number, and LAN ID
13	**Transit Management**	First Name, Last Name, Smartrip Card number, Workforce ID, Work Email Address, Home address, Work Phone, and LAN ID
14	**Transit Subsidy Program Enrollment**	First Name, Last Name, Work Force ID, and Home Address
15	**USA Performance**	First Name, Last Name, Middle Initial, Email, SSN, Work Force Id, and Work Phone Number
16	**User Management**	First Name, Last Name, Middle Name, Work Email, Work Phone Number, and LANID
17	**Lab Management**	First Name, Last Name, Middle Initial, Work Email Address, DOB, and Phone Number

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

Source of information is OASIS user community and Human Resources Line-of-Business (HRLOB) System. Information provided to USAP also comes from HRLOB. Information is collected using OASIS application specific, web-based user interfaces and/or secure share folders. OASIS receives a daily download of Federal employee information from HRLOB via a secure database link.

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, the system does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Role-based access is used to ensure only authorized users are allowed access. Application owners are responsible for providing users with training to ensure they are familiar with the application and enter data accurately. Due to information being provided by the employee or contractor, this ensures that the most relevant, up to data, and accurate information exist.

The HRLOB daily download ensures that OASIS has the most recent information and the most accurate information from Human Resource, which is the system of record for employee data.

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:

There is a risk that OASIS will retrieves more information than required from connected Information Technology (IT) system.

Mitigation:

The accuracy of OASIS data is dependent on the accuracy of the connected IT system information. OASIS is not the original point of collection for the information.

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, access controls levels are in place. Each OASIS application module has database role- base security and exercises the principle of least privilege so only the minimum required access rights are applied at the time of request. Access control levels and roles are different for each OASIS applications module. Authorized users are granted access to the OASIS application module based on their role.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Module owners are required to authorize access based on a business need. An access request form is submitted to the system owner on the behalf of the user and the required roles are assigned. Access roles are documented in the OASIS User Management Module.

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

No, there are no other components with assigned roles and responsibilities within the system.

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?

No external users for OASIS modules however Office of Human of Resource (OHR) USAP data is sent to OPM.

Internal parties include application owners, users, and contractors that provide web and database management support.

Yes, contractors accessing the system have the appropriate FAR clauses included in the contract.

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 information collected within OASIS is permanently maintained. The information is kept for the life of OASIS. Now that PSS2 is live, PSS1.0 data has been moved to PSS1 Archive and follows the existing OASIS record schedule.

OASIS follows EPA Record schedule 0740: Office of Administrative Services Information

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:

There is a risk that information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule.

Mitigation:

OASIS maintains all records with PII in accordance with applicable records retention or disposition schedules approved by NARA or based on the need and relevancy of the data in the support of the OMS mission. Some records are maintained as permanent records due to their continuing historical value; all other temporary records are disposed of in accordance with approved records schedules.

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.

Information is not accessible outside of EPA. The following modules do have requirements to share information to meet USA Performance requirements.

- HRLOB information is shared with OPM.
- The information is shared using an OPM provided API.
- The information is used for employee Senior Executive Services (SES) and NO-SES performance ratings.
- Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) apply.

In addition, OASIS serves as a pass through for Office Of Human Resource Strategy (OHRS) to share EPA information with the Office of Personnel Management (OPM) USAP System. EPA uses the OPM United States of America Performance (USAP) system to develop performance appraisals for both SES and Non-SES employees. EPA and OPM have developed and signed an ISA and a MOU.

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

External sharing of information to the organizations outside of EPA listed in 4.1 are for the purposes of completing a background investigation and obtaining a physical Personal Identification Verification (PIV) badge.

The information shared using the pass through to the USAP system is compatible with the original collection by the OHR as the information is used for the performance appraisals that are inherent to employment at EPA.

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?

Information that is shared within EPA and outside of EPA must have an authorized MOU and/or ISA in place before connections are granted. For inside the organizations, office directors authorize the use of data sharing via a MOU. Data is not shared unless both parties sign the required MOU/ISA. For outside the organization, a MOU/ISA is required to be in-place and signed by required signatories before connections are used. Also, the NPP should review all external agreements that share PII for reporting purposes.
For the OASIS pass through of OHR data to OPM's USAP application, EPA and OPM have developed and signed an Interconnection Security Agreement (ISA) and a Memorandum of Understanding (MOU).

4.4 Does the agreement place limitations on re-dissemination?

Limitation outlined within the contract discusses how the use of information is for the intended purposes. The MOU with OPM states that data provided to OPM shall not be re- disseminated or used except for the purpose intended.
For the OASIS pass through to USAP, the MOU states that the Privacy Act of 1974, governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

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:

Information shared outside the Agency for intended purposes as stated above. EPA connection to OPM for sharing USAP data is to occur over Transport Layer Security (TLS) 1.2. If this connection is misconfigured or comprised in any way, confidentiality of the data sent to OPM would be at risk.

For the OASIS passthrough to USAP, there is a risk that the information in the USAP system will be shared for purposes other than the stated purposes of the USAP program.

Mitigation:

PII data is sent to OPM over an encrypted channel for processing. MOUs and ISAs are in place with external parties to share information and provide required services.

This risk is mitigated because the system is not designed to share information between its users or the participating agencies, or otherwise outside of OPM. The system design and access controls ensure that USAP information is available only to authorized users who have registered with and have been granted a role based privileged accounts

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 as stated in Section 6.1?

OASIS ensures that the information is used for its intended purposes by incorporating role- based security which limits access to the information accessed or collected. Application and database auditing is enabled.

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

Employees and contractors are required to complete the EPA Annual Information Security and Privacy Awareness Training. A Rules of Behavior (ROB) form contains a detailed list of standards governing the appropriate use of the information system. Prior to accessing OASIS, users are required to read and acknowledge the agency's national rules of behavior (ROB), this acknowledgement effectively holds users accountable for their actions. OASIS users are required to read and acknowledge the agency national ROB annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Improper auditing.

Mitigation:

OASIS audit logs are reviewed per agency policies. In addition, OASIS audit logs capture is automated and reported daily. Each OASIS user must read and acknowledge the agency national Rules of Behavior (ROB) upon first use and annually thereafter.

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.

OASIS purpose is to provide uniform data storage and access for several personnel and asset-related processes. This takes the form of an intranet-based portal to several "modules," each of which represents a distinct business function and dataset. Refer to the OASIS software modules above for its intended purpose.

Information sent to OPM from OASIS is used to develop performance appraisals for both SES and Non-SES employees.

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 National Security Information (NSI) module can retrieve information by SSN. Other modules require one or more of the following fields to retrieve records: Name, Work Force ID, LAN ID, Personnel ID, Email Address, Smart Trip Number, Incident Number, Business Service Desk (BSD) Ticket Number, Asset ID, or Project Number.

Office Administrative Services Information System (OASIS), EPA-41 provides SORN coverage to OASIS.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

OASIS, EPA-41 SORN was conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records.

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:

For information passed through to USAP, there is a risk that authorized USAP users will export information from USAP and store the information on local hard drives or shared drives, putting it at risk for improper use and exposure.

Mitigation:

This risk is mitigated by use of access controls that restrict user access. Only designated HR administrators have permissions to export information from the system as needed at their respective agencies for an authorized purpose. In addition, all USAP users are required to adhere to USAP Rules of Behavior that govern the appropriate access and use of the USAP system.

*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.

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

Information collected is based on statutory requirements. Individuals do not access OASIS directly. Completion of OPM form OF-360 for Federal Employees and completion of the eFile information for Non-federal employees is not mandatory but required for employment at EPA. A Federal and non-Federal candidate may opt out of sharing their information.

For the pass through to USAP, EPA makes the decision concerning whether they will require their employees to use USAP to complete the performance evaluation process. As with a paper-based process, some individuals may decline to acknowledge the review completed by their supervisor or may refuse to use the system. In those instances, USAP allows supervisors to complete an employee's performance plan and the information contained in the plan will be communicated to the employee during meetings with his or her supervisor.

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.

Both Federal and non-Federal individuals are provided notice when they provide information via OPM's Electronic Questionnaires for Investigations Processing (e-QIP). The purpose of privacy information collected is to determine if background check is required and if so, complete that process. Background checks must be favourable for a person to commence work at the EPA.

Privacy Risk:

For the pass through to USAP, there is the risk that individuals were not provided notice concerning how the information they and others provide about them will be used.

Mitigation:

USAP cannot ensure that this risk is fully mitigated but each participating agency can mitigate this risk by ensuring that their performance plan templates contain appropriate Privacy Act statements. In addition, USAP has a dedicated help desk that users can avail themselves of to address questions and concerns and makes a list of Frequently Asked Questions available to users online.

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?

Individuals seeking access to information in this system of records about themselves are required to provide adequate identification (e.g., driver's license, military identification card, employee badge or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

For the pass through to USAP, the USA Performance Program Office provides employee users with login credentials so that they can register with USAP and access their performance plans. Users may also contact the USAP Help Desk if they need assistance with logging in. In addition, EPA employees will contact OHR to obtain information about them that is kept in the USAP system.

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

Requests for correction or amendment must identify the record to be changed and the corrective action sought. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16.
For the pass through to USAP, to update information in USAP, agency administrator users may log into the system, select the Update Personal Information option, and submit their

updates. An agency's HR administrators or an individual's supervisor may also correct data as needed, consistent with system performance policies, assigned role and Rules of Behavior.

8.3 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 risk that individuals may not know what procedures exist on collecting or correcting information.

Mitigation:

This Privacy Impact Assessment and the System of Records Notice provide information on the redress provisions available to individuals. Further, because much of the data the OASIS maintains is originally from other source systems (HRLOB for example), OMS/EASD relies on the notice of redress provisions of those systems to provide sufficient information to individuals.

Regarding USAP, users are provided with the capability to update their information online via the USAP website. USAP implements user access control such that an individuals can only access specific information pertaining to them. Participating agencies and OPM provide training to their individual users regarding the use of USAP as a self-service portal for viewing and submitting changes to performance documentation.