United States Environmental Protection Agency

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 Roster.docx

System Name: Office of Site Management and Operations Research Triangle Park General Support System (OSMO-RTP-GSS)		**System Owner:** Chanya Harris	
Preparer: Donald Anthony		**Office:** OFA-OCFSO-BSMD-BSOB	
Date: 4/29/2026		**Phone:** (919) 866-8469	
Reason for Submittal:			
New: ☐	Revised:☐	Annual Review: ☒	Rescindment: ☐

System Lifecycle Stage(s):		
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐
Operation & Maintenance: ☒	Rescindment/Decommission: ☐	

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:

In pursuing its mission, information system uses a networked infrastructure to provide the data processing needs to employees, contractors, and partners. This infrastructure includes both hardware and software to support both mission and daily operations. This general support system (GSS) contains or connects to the US EPA's Wide Area Network (WAN), as well as minor applications. The components of the OSMO-RTP-GSS make up the central hardware and software that provide connectivity, security, storage, and data access for agency employees and contractors. These range from client devices, where employees and contractors can do daily work, to central data storage and management devices. Many of the components of the OSMO-RTP-GSS are the physical tools or systems used to implement the security controls: access control systems provide a mechanism for moderating access requests to information, remote access devices appropriately limit access to systems to a distributed workforce, boundary protection devices protect internal systems from unauthorized access.

Section 1. 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?

Executive Order 12072 (Aug. 16, 1978), Federal Property and Administrative Services Act of 1949, 40 U.S.C. 121, and Executive Order 9397 (Nov. 22, 1943). 42 U.S.C. 290dd-1, 290ee-1; 5 U.S.C. 7901; Executive Order 12564 (Sept. 15, 1986). Office of Federal Procurement Policy Act of 1974, 41 U.S.C. 414. Public Law 107-67, Section 630, and Executive Order 9397. 5 U.S.C. 1104, 5 U.S.C. 1302, 5 U.S.C. 3301, 5 U.S.C. 3304, 5 U.S.C., 3320, 5 U.S.C. 3327, 5 U.S.C. 3361, and 5 U.S.C. 3393. The Telework Enhancement Act of 2010 (December 9, 2010); Public Law 111–292.

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?

The system has a valid and approved System Security Plan (SSP) and has been issued a continuous Authorization to Operate (ATO) by the Authorization Official (AO). The memo was signed 10/30/2025. The ATO expires 10/22/2026.

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.

Information contained in the system is administered in accordance with all applicable federal laws, including the Paperwork Reduction Act (PRA), the Privacy Act of 1974, and EGovernment Act of 2002. 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?

Yes. The system stores backups of all data on the US EPA's instance of Microsoft Azure. The Platform-as-a-Service (PaaS) offering is FedRAMP approved.

Section 2. 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).

The OSMO-RTP-GSS system does not directly collect personal information (PII). Employees can save work-related documents on different servers. These documents may include all types of information the Agency uses, such as investigations, consumer complaints, supervision records, HR data, and other information needed for the Agency's work. Sometimes, this information contains PII about employees, contractors, consumers, people working for supervised companies, and others. The PII can be basic, for example, names and contact details (such as email or phone number), or more sensitive, such as Social Security numbers or bank account details. Information is stored as PDF files or word processing and spreadsheet documents. There is no special app or database that collects or keeps PII. The OSMO-RTP-GSS Privacy Impact Assessment (PIA) covers all this information that is stored on or passes through the Agency's systems.

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

The information collected is typically provided by the individual or employee. In cases where information is not obtained from the individual or employee, the Agency collects such information in accordance with applicable laws and pursuant to applicable agreements governing the sharing of such information (e.g., Memoranda of Understanding, Memoranda of Agreement)

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

OSMO-RTP-GSS does not use information from outside sources. The OSMO-RTP-GSS is a collection of servers, routers, network appliances, and infrastructure equipment. It's not a database that uses data from another source, and it's not an application that would reference any external information. Its only purpose is to host/store agency data.

2.4 Discuss how accuracy of the data is ensured.

The OSMO-RTP-GSS is only responsible for storing and backing up data, which is hosted there, but the accuracy of that data is only measurable by specific Data Owner(s) or Points of Contact (POC's).

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 primary risk to the characterization of the data is human error, which could result in the collection of inaccurate data.

Mitigation:

Mitigations to protect Privacy include National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) technical, physical, and administration controls. Privacy controls are audited on an annual basis for efficacy. The users of the information are provided privacy, security, and Rules of Behavior training on an annual basis. The Agency has a Chief Information Officer (CIO), Chief Information Security Officer (CISO), Information System Security Officer (ISSO), and Privacy Officer (PO) on staff to assist and monitor in protecting the individual's information. Users of the information are only given access to records that are needed to complete their duty tasks.

Section 3. 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?

The minimum-security requirements for our moderate impact system cover seventeen security related areas regarding protecting the confidentiality, integrity, and availability of information systems and the information processed, stored, and transmitted by those systems. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The OSMO-RTP-GSS employs all security controls in the respective moderate impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in the NIST Special Publication (SP) 800-53 and specific EPA directives.

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

The access control levels are documented in the SSP, User's Guide, and Standing Operating Procedures (SOPs). Role-Based Access Controls (RBAC) are in place to ensure that information is accessed in accordance with the uses described above. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Users of the information system are only given controls to access the information that is essential and pertinent to complete their duty assignments. This is accomplished through strict adherence to EPA CIO Policy CIO 2150-P-01.2 “Information Security – Access Control Procedure”, as well as, technically enforced with implementation of Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) related to NIST control AC-6 “Least Privilege.” The information contained in the system is relevant to the mission of the EPA. Any violations of access or use of the information are investigated by the PO and Information Security Officer (ISO) and referred to the supervisor and Human Resources (HR) for disciplinary action.

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?

An individual is assigned the type of access they need to complete their duty tasks. The supervisor maintains a functional category form on employees that is reviewed annually. Monitors and audits are completed on the functional categories by the supervisor and ISO. Contractors that have access to the computer system are only delegated functions needed to complete their duty task. They are required to complete annual privacy, security, and Rules of Behavior training. Contracts are reviewed on an annual basis by the Contracting Officer Representative (COR). The PO and ISO monitor that the annual privacy, security, and Rules of Behavior training are completed by contractors and business associates. The OMS-OSMO IT Support and Infrastructure Services (ITSIS) contract outlines the privacy clauses in accordance with the Federal Acquisition Regulation (FAR). The contract vehicle for the information system support includes FAR (48CFR) clauses 24.104 and 52.223 clauses 1 and 2.

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 OSMO-RTP-GSS is only responsible for storing and backing up data, which is hosted there. Individual data owners are required to follow Agency standard record management policies and procedures. The OSMO-RTP-GSS does not assume ownership of any data stored on the information system servers.

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 information retained could be subject loss, or unintentional destruction from external, internal, and physical risks.

Mitigation:

The Records Manager and Alternate Records Manager ensure data retention policies and procedures are followed. The CISO, ISO, ISSO, and PO monitor controls to mitigate any breaches of security and privacy. Building Systems Operations Branch (BSOB) system support-staff backup the data daily in case human error leads to accidental deletion.

Section 4. 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.

OSMO-RTP-GSS does not share data with any outside entities. The extent of which data owners share information and with whom the information is shared, and the method of sharing will vary based on their specific mission or operational use. The Agency may share information when working with other Federal or State governmental agencies for purposes of enforcing various related laws or regulations.

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

The OSMO-RTP-GSS is only responsible for storing and backing up data, which is hosted there. The information system does not share any information with external information systems. It is solely designed as a platform to host data on.

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?

US EPA policy requires that any connections from the information system to other information systems must be documented in an Interconnection Security Agreements (ISA). For connecting systems that have the same Senior Information Official (SIO), an ISA is not required. Rather, the interface characteristics between the connecting information systems shall be described in the SSP for the respective systems. Any ISA or Memorandum of Understanding/Agreement (MOU/A) must be reviewed, approved, and signed by the ISO. MOUs are reviewed by Local Privacy Officer and the Agency Privacy Officer following internal procedures prior to issuing.

4.4 Does the agreement place limitations on re-dissemination?

Currently there are no shared agreements in place.

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. OSMO-RTP-GSS does not share any information. It is simply a platform to host data on.

Mitigation:

None. OSMO-RTP-GSS does not share any information. US EPA policy requires that all individual data owners assume responsibility to protect their data and follow standard procedures when sharing data.

Section 5. 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?

Through implementation of NIST administrative and technical privacy controls, the information system ensures the PII is only used for the authorized purpose(s). The information system implements technology to audit for security, appropriate use, and loss of PII. The system enforces an RBAC scheme to ensure that only the personnel required to view or use the information stored on the system have access. The OSMO-RTP-GSS is configured to set access permissions and audit critical directories and files. The information is configured to bind the identity of the information producer with the information. The system is configured to provide the means for authorized individuals to determine the identity of the producer of the information.

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

All US EPA personnel and contractors are required to take Information Security and Privacy Awareness and Rules of Behavior Training(s) annually.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Discuss the privacy risks associated with the technical and policy-based safeguards and security measures. How were those risks mitigated?

Privacy Risk:

There is a potential risk of failure to log anomalies and notify system personnel in the event of misuse.

Mitigation:

The Agency minimizes this risk by enforcing access controls to minimize the number of individuals who have access to the data and by storing data on systems that have been accredited as secure for this type of data. Automated tools are employed within the environment to indicate potential misuse of information. The information system components are monitored by SPLUNK to audit activity within the environment. SPLUNK logs are sent to the Computer Security Incident Response Capability (CSIRC) information system who manages the Security Incident and Event Management (SIEM) tool ArcSight which normalizes audit events and reports on any detected unusual or inappropriate activity. Additionally, the system also employs various tools to provide a unified audit trail identifying all data the has been created, opened, modified, or deleted and by whom. Finally, all logs are backed up daily.

Section 6. 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

List each use (internal and external to the Department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

The information covered by this PIA is used to support all Agency's mission and operation objectives, including the Agency's enforcement, supervision, consumer response, market research, consumer education, and operational activities. As the primary IT infrastructure used by the US EPA, Information in the OSMO-RTP-GSS is collected, used, disseminated, and maintained for the Agency to perform its policy, personnel management, and other activities. Facilities Management maintain financial information in the OSMO-RTP-GSS for the procurement of goods and services and to support internal operations of the agency. BSOB security personnel capture and review system audit data. Human Resources staff often utilize designated folders on shared drives within the Information System to store employee and contractor data for personnel management activities. Additionally, Human Resources staff preserve some archival data from other systems maintained by the US EPA. Information regarding the purposes of information collected by the other various systems can be found in the specific PIAs for those systems.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☐ 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 OMS-RTP-GSS is only responsible for storing and backing up data which is hosted there and is not designed to retrieve information. The OMS-RTP-GSS provides only the operating system and hardware to store data.

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?

The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.

The Agency minimizes this risk by enforcing access controls to minimize the number of individuals who have access to the data and by storing data on systems that have been accredited as secure for this type of data. Staff are also trained in how to handle potential breaches to minimize negative impacts. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Users of the information system are only given controls to access the information that is essential and pertinent to complete their duty assignments. This is accomplished through strict adherence to EPA CIO Policy CIO 2150-P-01.2 "Information Security – Access Control Procedure", as well as, technically enforced with implementation of DISA STIGs related to NIST control AC-6 "Least Privilege". The information contained in the system is relevant to the mission of the EPA. Any violations of access or use of the information are investigated by the PO and ISO and referred to the supervisor and HR for disciplinary action.

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:

There is a risk of unauthorized access and misuse of data elements in the system.

Mitigation:

Only select personnel and a very limited set of BSOB support contractors have access to and will use the consolidated information stored in the system. The following NIST controls for privacy have been implemented and reviewed by the EPA National Privacy Program for feasibility and acceptability: Authority and Purpose, Accountability, Audit, and Risk Management, Data Quality and Integrity, Data Minimization and Retention, Individual Participation and Redress, Security, Transparency, and Use Limitation.

STOP HERE.

The National Privacy Program (NPP) will determine if a System of Records Notice (SORN) is required. If so, the following additional sections will be required.

Section 7. 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.

Click or tap here to enter text.

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?

Click or tap here to enter text.

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:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.

Section 8. 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?

Click or tap here to enter text.

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

Click or tap here to enter text.

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 Freedom of Information Act (FOIA).

Privacy Risk:

Click or tap here to enter text.

Mitigation:

Click or tap here to enter text.

I attest as the Agency Privacy Officer that **Office of Site Management and Operations Research Triangle Park General Support System (OSMO-RTP-GSS)** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.09.04 14:56:43 -04'00'

Lee Kelly
Agency Privacy Officer
Cybersecurity Planning & Risk Mgmt. Branch
EPA/OFA