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: Contract Laboratory Program Support System (CLPSS)	**System Owner: Renee Hamilton**
Preparer: Renee Hamilton	**Office: OLEM/OSRTI/TIFSD/ASB**
Date: May 17, 2021	**Phone: 703-603-9092**
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 Contract Laboratory Program Support System (CLPSS) provides centralized, automated support of processes inherent in the collection, analysis, evaluation, reporting, and payment of samples and analytical chemistry services under the Contract Laboratory Program (CLP). CLPSS also maintains database and tracking systems to track performance of analytical methods, provide data for Superfund cost recovery, monitor laboratory performance, and maintain laboratory contract and invoicing information. In addition, CLPSS is used to distribute electronic analytical data for use in Regional programs and ASB research studies. The CLPSS is a FISMA reportable contractor system housed, run and maintained on the Sample Management Office (SMO) Contractor-provided Information Technology (IT) infrastructure, servers, and software in Bossier City, LA. All the primary and subsystem operating components of CLPSS are owned

by the EPA.

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?

ASB manages and supports the Contract Laboratory Program (CLP). The CLP is a national network of commercial laboratories and support contractors whose fundamental mission is to provide data of known and documented quality. The CLP supports EPA's Superfund program, created under the 1980 Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), and currently under the 1986 Superfund Amendments and Reauthorization Act (SARA). The collection of information by CLPSS was covered under the following contract clauses: Treatment of Confidential Business Information (EPA AR 1552.235-71) (APR 1984) & EPA AR 1552.235-76 (APR 1996); Release of Contractor Confidential Business Information (EPA AR 1552.235-79) (APR 1996) AND Access to Confidential Business Information (EPA AR 1552.235-80) (OCT 2000) CLPSS provides centralized, automated support of processes inherent in the collection, analysis, evaluation, reporting, and payment of samples and analytical chemistry services under EPA's Contract Laboratory Program (CLP). The Office of Environmental Information Policy's EPA classification No: CIO 2134.0 establishes objectives, responsibilities and procedures for preparation, review and clearances for Agency efforts to collect or obtain information from the public in support of the Agency mission.

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, there is a CLPSS Security Plan. The system was first granted the Authority to Operate (ATO) in November 2002; the accreditation was valid for three years and was re-accredited every three years or whenever a major change occurs. CLPSS obtained continuous ATO since November 2002 until now. The last ATO was granted on December 6, 2019 and will expire on December 6, 2022.

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?

At this time CLPSS and its data is NOT hosted/stored in the Cloud. In the future, EPA ASB may consider having a CLPSS disaster recovery site in a FedRamp approved AWS or Microsoft Azure using IaaS service.

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).

Data collected, used, disseminated, or maintained by the system is CLP Laboratory Contract data, sample data, and analytical data. CLPSS maintains database and tracking systems to track performance of analytical methods, provides data for Superfund Cost Recovery, monitors laboratory performance, and maintains laboratory contract and invoicing information. CLPSS collects the name of the person, work email address, and work phone number for all users requesting access to the system, in order to create the user account. No other PII is collected or maintained by the system.

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

The sensitivity of data exchanged is Confidential Business Data related to the CLP Laboratory and not classified as sensitive. There is no Personally Identifiable (PII) data being transmitted with the system.

CLP Laboratory Contract data is entered from the Laboratory contract awarded by EPA into CLPSS. This data is collected to be used in scheduling samples. The laboratory sample data (sample numbers assigned to each sample collected for analysis) is provided by the EPA Regional samplers. The Laboratories analyze the samples and submit their analytical data electronically using CLPSS. This information is used by the Laboratories to create and submit their invoices in CLPSS for processing and transmission to EPA for approval and payment.

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.

The CLPSS application, where possible, provides drop-down lists to limit the possibility of someone entering inaccurate information. Fields that require manual entries perform authentication checks, such as format matching for dollar amounts and exceeding funds available. CLPSS organizational data that is collected in the system is not sensitive and changes to any data in CLPSS is controlled by the user. The SMO Contractor maintains procedures to give data subjects reasonable access to data as appropriate, as well as the

ability to correct, delete, or update inaccurate or incomplete information. Also, there is a specific CLPSS function/application (EXES) that performs automated quality control checks on CLP laboratories electronic deliverables to ensure accuracy of lab analytical data.

2.4 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 potential exposure to PII information.

Mitigation:

Follow PII privacy controls that are set in place in the CLPSS Security Plan.

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?

All accounts are separated into roles. The roles have varying functions from general users up to administrative rights to prevent misuse. Users are only provided the rights necessary to perform their jobs. Access to data within the application is controlled by access controls specific to a role, and all users are assigned to specific roles. The most restrictive rights are developed for system access and granted with respect to least privilege at the functional level for maintaining the operation of the system, as well as within the application, for using the system. For example, you must register and accept the terms and agreement before gaining access to applications or functions. The organizations can manage their profile and any information is updated and reset by the organization user after they are approved and granted access to the system. All SMO users that have access to CLPSS must have an active Position of Trust.

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

The SMO CLPSS Portal User Management Standard Operating Procedure (SOP), SIS-3 describes how access is granted and controlled within CLPSS for CLPSS Users. Users can request access to the SMO CLPSS Portal and are assigned particular applications within the system based on their organization. The SMO CLPSS Help Desk Data Administrator (DA) will follow the procedures outlined in the SOP when approving or rejecting Users for access to applications. Once Users are approved by the EPA System Owner, the SMO CLPSS Help

Desk DA is also responsible for managing the User accounts and any account modifications. Users who are performing work for the EPA may request access to the SMO CLPSS Portal. Access within the SMO CLPSS Portal will be restricted based on the User's organization and associated applications. A User is approved once their profile and requested applications have been reviewed. All staff accessing the network will be required to read the Rules of Behavior and acknowledge they accept the terms when registering for an account to CLPSS through the SMO CLPSS Portal before they are issued a user ID and access to the system. All SMO contract support personnel are also required to attend regular Security Awareness Training related to their work function. The Rules of Behavior are based on Federal laws and regulations and EPA directives**.**

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

Yes.

The most restrictive rights are granted with respect to least privilege at the functional level for maintaining the operation of the system, as well as within the application, for using the system. Accounts are separated into roles and groups and the system prevents non-privileged users from executing privileged functions based on their role and within a defined group.

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?

EPA personnel and contractors have access to CLPSS data. Contractors include: CLP Laboratories, CSRA-SMO Contractors.

The appropriate Federal Acquisition Regulation (FAR) clauses are included in the EPA Sample Management Office (SMO) contract. Examples of contract clauses incorporated in the SMO contract by reference are: Project Employee Confidentiality Agreement (EPAAR 1552.227-76) (MAY 1994); Treatment of Confidential Business Information (EPAAR 1552.235-71) (APR 1984) & EPAAR 1552.235-76 (APR 1996); Release of Contractor Confidential Business Information (EPAAR 1552.235-79) (APR 1996) and Access to Confidential Business Information (EPAAR 1552.235-80) (OCT 2000).

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.

Hard copy of laboratory analytical data and related hardcopy deliverables are stored at the EPA Federal Records Center (FRC). Hard copy data is retained at FRC for 30 years. The reason for retaining this information is for Cost Recovery of Superfund sites. CLPSS is under EPA Records Schedule 0089 (Title: Information Tracking Systems; Status: Final, 05/31/2017; NARA Disposal Authority: DAA-GRS-2013-00020016)

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 privacy risk is the potential of keeping records longer than their actual retention timeframe.

Mitigation:

The mitigation is that the record schedule is followed.

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

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

There is no external sharing of CLPSS data outside the 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?

For organizations within EPA, an Interconnection Security Agreement (ISA) exist between CLPSS and Contract Payment System (CPS). Invoice data is exchanged between the two systems and data transmitted is Confidential Business Data related to CLP Laboratory data. The sensitivity of data exchanged between US EPA and the SMO Contractor is Confidential Business Data related to CLP Laboratory and not-classified as sensitive. There is no (PII) data being transmitted or linked which reduces the sensitivity and reduces the risk resulting from disclosure. EPA system users are expected to protect CLPSS database and CSRA system users are expected to protect CPS database in accordance with the Privacy Act & Trade Secret Act and the Unauthorized Access Act.

4.4 Does the agreement place limitations on re-dissemination?

No

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. There is no external sharing.

Mitigation:

N/A

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?

Laboratories are assigned unique laboratory codes when their contracts are awarded and when they are provided access to CLPSS to submit their analytical data and invoices. Their access of CLPSS is managed through the user management component of CLPSS. The laboratories register using unique IDs and passwords according to CLPSS password rules and are only granted access to their data.

EPA has an established Privacy Policy 2151.0 which establishes the National Privacy Program for EPA which provides national oversight for administering and ensuring EPA's compliance with its requirements under the Privacy Act of 1974, the E-Government Act of 2002, the Federal Information Security Management Act (FISMA) and policy guidance issued by the President and Office of Management and Budget (OMB). This Policy applies to all EPA employees, managers, contractors, and grantees working on behalf of EPA who handle, control, or access documents, records, or information technology (IT) systems that contain Privacy Act and personally identifiable information. In addition, the SMO Contractor has a Director who is responsible to implement privacy policy, to promulgate additional privacy policies as required, and to coordinated privacy related compliance and other services and resources to employees and stakeholders.

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

The SMO Contractor has a Chief Information Officer (CIO) and notice is sent annually from the CIO to complete annual Cyber Security & Personal Data Privacy Awareness training. Completing this training course is required by all SMO Contractor employees to meet regulatory compliance. The course provides valuable information on understanding and protecting yourself from common security threats; identifying Personally Identifiable Information (PII) and understanding the importance of protecting it; and recognizing the signs of insider threat and what to do about it. At the end of the course employees are asked to read and acknowledge the SMO Contractor's User Access Agreement and Standard. The SMO Contractor's Ethics and Compliance Office (ECO) is responsible for ensuring and administering the policy, for auditing compliance and for investigating violations of the policy. The SMO Contractor collects and documents privacy awareness

training records. These records can be provided as required to higher authorities and EPA. In addition, privileged SMO users have to complete a mandatory annual EPA Information Security and Privacy Awareness Training. This training course is accessible through "FedTalent" on the "One EPA Workplace" site.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Low risk of untimely/improper review

Mitigation:

Account restrictions and controls exist within the system. There are limited access rights depending on user role. The PO during his/her review will ensure that the information is being properly used.

Section 6.0 Uses of the Information

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

6.1.A Describe how and why the system uses the information.

The CLP laboratories provide data which can be used for a variety of purposes including defining the nature and extent of contamination at Superfund sites. Supporting documentation regarding costs of these services needs to be provided quickly because of cost recovery activities associated with Superfund litigation.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes___ No_X__. 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.*)

Data is retrieved by a unique ID/Tracking group ID number generated by the system as data is submitted by the CLP Laboratory.

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?

All CLPSS Users only have access to their data. No one else has access or sees their data other than the SMO Contractor to perform official duties. The data is only used for the intended purpose as laboratory analytical data is reviewed and the analytical results are provided to the laboratory and the Regional client where the samples originated. Laboratories invoice for their analytical data through CLPSS and this data is only viewed by the Regional Invoice Approving Official for invoice approval, SMO Contractor for review and recommendation of the invoice, and EPA upon review and payment of the

invoice.

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:

The information might be misused

Mitigation:

There are limited access rights depending on user role. The PO during his/her review will ensure that the information is being properly used.

***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.

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?

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:

Mitigation:

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?

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

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:

Mitigation: