United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 07/2018)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf.

If you need further assistance contact Patricia Brooks, at brooks.patricia@epa.gov (202) 564-3717.

System Name: CLU-IN System (CLU-IN Contractor LAN)	
Preparer: Michael Adam	**Office: OLEM OSRTI TIFSD TIIB**
Date: 2/13/2019	**Phone: 703-603-9915**
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 Contaminated Site Clean-Up Information (CLU-IN) System provides information about innovative treatment and site characterization technologies to the hazardous waste remediation community. It describes programs, organizations, publications, and other tools for federal and state personnel, consulting engineers, technology developers and vendors, remediation contractors, researchers, community groups, and individual citizens. The site was developed by the U.S. Environmental Protection Agency (EPA) but is intended as a forum for all waste remediation stakeholders.

CLU-IN users include internal customers within OSRTI as well as external users within other Agency offices (both headquarters and regions), other federal agencies, state and local governments, private sector organizations, the general public, and international organizations. Most of these users are browsing anonymously on the website. Some partners we share event registration information with. This business contact information is controlled with passwords, rules of behavior, and does not contain sensitive PII. CLU-IN provides information on the topics listed above through the use of online reports, email

newsletters, webinars, videos, conference webcasts, technology selection tools, site-specific profiles of technology applications, and links to other online resources. While CLU-IN primarily serves as an instrument for information dissemination, it does receive, and process user-supplied information related to site-specific profiles of technology applications and registrations for online events hosted on CLU-IN.

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 need for the Library and the Cleanup and (National) Response training provided for or listed (registration and registration management) via the System is defined by:

- CERCLA Section 311(b) (8) & (9);
- National Oil and Hazardous Substances Pollution Contingency Plan Overview (NCP), Section 300.120 (h) (1), and Section 300.145(b) (3);
- HSPD-5 (NIMS) (https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf)
- The Gold King Mine After Action Report: defined the need for a National Incident Management Assistance Team

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, this system was last authorized to operate on August 24, 2015. A new ATO package is in final review for a FedRAMP Authorized Virtual Private Cloud instance (meaning the System as-is described but modified to work on a Cloud server instead of the current contractor-server instance), which includes a draft final ISSP from April 2018.

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?

Yes, pending the ATO approval for the Cloud instance of the current system. The Cloud is an IaaS.

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).

The system collects common business contact information, which may include name, business phone number, business email, organization, business address, job title, job description, and supervisor contact information. The specific data elements collected depend on the audience and delivery mechanism of the course/information.

Other data is technology information about remediation of hazardous-waste sites, including some submitted technical information regarding technologies used at sites for case studies. For context, it also provides information on how to use them and links to relevant guidance established by Federal, State, and in some instances, Tribal governments, workgroups, and consortia. Products on the sites include technical reports, databases (case studies), archives technical seminars, technical periodicals (newsletters), narratives on Best Management Practices, and focused narratives describing technologies, strategies, and issues for cleaning up sites. This technical data does not contain Agency records (that are not stored elsewhere as records). It does not provide automated manipulation scientific data.

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

All information is user-supplied through online forms over an HTTPS-only connection in compliance with Office of Management and Budget memorandum M-15-13.

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

The system is primarily an informational website that contains (or links to) government reports, technical literature, technical narratives, conference proceedings, site profile databases; some of which may have PII but is already public domain, and/or designed for public access; which is to say, the intent is not to protect that PII because it is meant to be public (authorship and/or contact information on an output, like a journal article, or government report, for example), nor is the focus the collection of the PII, the PII is there intentionally for the public and tangent/additional to the utility of the technical information.

This is N/A for the purposes of course registration. Registration information with PII is not public.

2.4 Discuss how accuracy of the data is ensured.

All collected PII is user-supplied information to the greatest extent practicable. The confirmation of the accuracy, relevance, timeliness, and completeness of this PII is limited to ensuring all required fields are completed and valid email address syntax through automated validation included with online forms. Any change to PII information is collected directly from the user, through the email system provided by the user. System Owners update information in systems, forms, and databases (If Applicable) and informs the National Privacy Program of needed changes. No other user-supplied information (for the purpose of course registration) is reviewed further for accuracy, relevance, timeliness, and completeness. Users update their information as needed.

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:

Risks include (business) contact information used for course registration and rosters.

Mitigation:

□ PII that is meant for public consumption (contained within public, technical content, example: authorship contact information) is not protected, it is a public website designed for public access.

□ PII that is used for registration and roster purposes is protected by Controls intended for privileged (administrative: contractor only); EPA and Organization partners have access to rosters for the purposes of managing/implementing for only the courses they offer with "read" only access. Participant users only have access to their own information and only through an email account they provide, but those email systems are outside the system boundary (users must know their email passwords from whatever email system they use/choose to access their registration history).

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 to view information is limited to contractor support staff and EPA employees and controlled through individual accounts that are verified, approved, established, activated, monitored, modified, disabled, removed, and retained on file by the contractor system manager as account manager. Only contractor support staff with Environmental Management Support

(EMS), Inc. have “privileged” accounts to modify and delete information (at the direction of EPA TOCORs).

The information is only shared with EPA Task managers, EPA contractors with Admin rights, and those who are “sponsoring” (the office or organization) the training. However, the organizer/sponsor and EPA TOCOR/Alt TOCOR may see the roster information. The roster information is not public.

Technical Class Controls (for Admin accounts, “Users” do not have privileged accounts, they can only “retrieve” their course history and information via email, and submit requests to have their information changed, they cannot automatically change or receive information via the system (browser) nor can they access other’s PII. The bulk of the system is designed for public technical information dissemination via anonymous public access and does not contain PII that is not already public and “designed” to be public, for example: authorship)

- Access Controls:
  - Account Management
  - Access Enforcement
  - Least Privilege
  - System Use Notification
  - Session Lock
  - Supervision and Review -Account Management
- Audit Controls:
  - Auditable Events
  - Audit Analysis, Monitoring, and Reporting
- Identification and Authentication

Management Class Controls

- Security Planning, Policy, and Procedures
  - Rules of Behavior
- Privacy Requirements for Contractors
  - All contractors and service providers who have access to PII stored within the system operate under support contracts that include FAR clauses 52.224-1 and 52.224-2 referenced in 24.104.

Operational Class Controls

- Security Awareness and Training Policy and Procedures
  - Security Awareness
  - Security Training

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

“Users” do not have privileged accounts, they can only “retrieve” their course history and information via email, and submit requests to have their information changed, they cannot automatically change or receive information via the system (browser) nor can they access other’s PII. We have Rules of Behavior for both of these accounts with access that are signed and explained (in a meeting) annually. The most recent annual forms and Rules are in the ISSP Appendix.

Account management procedures are defined in system security plan (ISSP). The contractor system manager maintains accounts and access privileges. Each user account is provided with an access role appropriate to that user's role and responsibilities. The access role defines whether information can be accessed, and what can be added, modified, and deleted. Any system access granted to contractor support staff is dependent on compliance with confidentiality requirements of the support contract and compliance with the system rules of behavior. Only EMS has privileged accounts, other course management (EPA included) have only read-only access. These are used only by TOCOR and Contracting support, this "account" role does not apply to "users" they can only retrieve information related to their own training records for themselves and only via an email account of their choosing.

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

No. The course rosters (the PII) reside on Trainex.org and Cluin.org (both are within the CLU-IN System) for the purposes of training, but the System Infrastructure and practices for safeguarding the information are the same.

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?

Access is limited to CLU-IN System support contractors and EPA Task Order Managers responsible for managing relevant support contracts, including:

- Environmental Management Support (EMS), Inc. under EPA Contract No. EP-W-13- 016, Task Order 0002, including clauses 52.224-1 and 52.224-2 referenced in 24.104. *EMS is the only contractor with Admin (read/write) priviledges.
- Tetra Tech, Inc. under EPA Contract No. EP-BPA-16-0004, Task Order - call orders: (EP-B165-00077 – EP-B165-00081), EP-B175-00020, and (EPB175-00036 – EP-B175-00038), including clauses 52.224-1 and 52.224-2 referenced in 24.104.
- ICF International, Inc. under EPA Contract No. EP-W-14-001, Task Order 01, includingclauses 52.224-1 and 52.224-2 referenced in 24.104.
- HazTrain, Inc. under EPA Contract No. GS-10F-0143K, Task Order EP-G15S-00150, including clauses 52.224-1 and 52.224-2 referenced in 24.104.
- Interstate Technology & Regulatory Council (ITRC)

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.

Information is retained as retrievable and usable records as long as necessary to conduct Agency business as described under EPA Records Schedule 0094 (Electronic Bulletin Boards), principally through registrant transcripts.

Other information that may contain information is derived from already public information and is removed when the information in the document is considered technically outdated. Material that may be out-dated by the cognizant EPA/Gov "Record" determination may be kept or removed for technical purposes independent of the Record since the System's technical information is not the Record depository for items deemed as Records (a copy of the "Record" is kept on the "Record" retainment System(s) designated for that 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:

Business contact information, course transcripts and roster information may be exposed.

Mitigation:

Users can only access through their supplied email and the information is not displayed or disclosed to them within the CLU-IN System. Course managers have access to roster information but do not have write privileges and are required to handle the information appropriated and informed (Rule of Behavior) about the proper use of information and information sharing on a annual basis.

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.

Partners access the information as course managers for courses they are providing to the public on our platforms. These courses are consistent with the purpose of the CLU-IN and Trainex audiences and EPA mission. All external sharing is based on compliance with signed copies of the CLU-IN System Information Sharing: Rules of Behavior, which are retained on file by the System Owner.

Yes. Information is shared with the following partner organizations outside EPA, only for the purposes of each to manage their own courses/events:

- National Institutes of Health, National Institute of Environmental Health Sciences, Superfund Research Program
- Interstate Technology & Regulatory Council (ITRC)
- U.S. Army Corps of Engineers
- Other Federal partners as needed who have relevant training that aligns with

EPA's site cleanup and response missions

Information is accessed through individual accounts for EPA Task Order Managers responsible for the CLU-IN system or contractor system support staff. This information is then provided to the relevant partner organization to manage an event, and analyze professional demographic characteristics of participants in the specific events they host.

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

The external partners use our training platforms to perform training that is consistent with the EPA OLEM mission. The collection is done in order for Users to register and attend the training course, seminar, or other live event.

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?

They are informed of the Information Sharing Rules of Behavior annually or at the moment they first use the system for their training.

Current, signed Information sharing agreements are manually reviewed on an annual basis by the system owner to ensure there is an ongoing business need for information sharing related to the management of courses/events sponsored by the relevant partner organization. New Information sharing agreements are approved by the system owner based on a demonstrated business need and compliance with the terms of the information sharing agreement. New uses of this information must conform to the information sharing agreement.

4.4 Does the agreement place limitations on re-dissemination?

Yes. It is not to be shared outside the purposes for the management of the training course or live event.

Current, signed Information sharing agreements are manually reviewed on an annual basis by the system owner to ensure there is an ongoing business need for information sharing related to the management of courses/events sponsored by the relevant partner organization. New Information sharing agreements are approved by the system owner based on a demonstrated business need and compliance with the terms of the information sharing agreement. New uses of this information must conform to the information sharing agreement.

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:

Some business contact information, and roster information may be exposed.

Mitigation:

Risk is mitigated through controls including Rules of Behavior that outline how to handle information securely and are reviewed with course managers and those with privileged access annually. The number of people that the information is shared with is limited to only those who are course managers.

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?

Privileged accounts are maintained by controls outlined in the ISSP. The System does not display PII publicly, only at the request of a User, and only via their email system (outside

The System boundary) and not within a web browser, for example.

Once rosters are not within the System boundary (they are being used by course managers for managing the course) they are not managed by the System.

Those with privileged accounts sign annually (training) a Rules of Behavior for the System that includes Privacy.

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

The annual system security training provided to contractor support staff and all EPA employees addresses PII, the Privacy Act of 1974, and the E-Government Act of 2002. Training completion for contractors with privileged (admin) accounts is verified through signatures provided to the EPA Task Order Manager; see Appendices of most current ISSP (Rules of Behavior).

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

Business contact information, course transcripts and roster information may be exposed.

Mitigation:

Account restrictions and controls exist within the system but do not exist outside of the System Boundary. For privileged account users (there are four EMS employees with privileged accounts), these controls exist:

- Authenticator/Password Management – logs and timed password change requirements
- Account Management – need to know; login failure logs,
- Access Enforcement -- Application and monitoring of access privileges.
- Least Privilege -- Provision of the minimum tools required for a user to perform his/her function. (Support contractors who do not operate the System have Read only)
- Unsuccessful Login Attempts
- Audit logs are reviewed on a periodic bases as described in the ISSP
- Audit logs have management and technical controls to preserve integrity of the logs

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 primary uses of user-supplied PII information are to:

1. Allow registrants to check in and record attendance for both webinars and classroom courses.
2. Distribute email newsletters that individuals opt in to receive.

EPA staff also use the information to analyze demographic characteristics of event participants.

It is in the Privacy Notice, but this is not unlike anonymized cookie analysis, though this is information like which Regions are attending the courses/events, which groups are primarily attending, industry/academia/Fed gov/State gov, which EPA Offices, etc. (https://clu-in.org/conf/itrc/register/privacy.htm)

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.*)

A provided business email address. The system does not display PII to Users. It sends information to the email address of record, and changes are made by requesting changes in response to this email. Personal identifiers cannot be used to retrieve and display information directly within the user's browser.

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

None.

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:

a. System collects Tier 2 persistent cookies

b. System has roster information on it, which contains PII, as business contact information but does not contain sensitive PII.

Mitigation:

Users may opt of cookies. We don't collect personal information in the cookies. We have Rules of Behavior and System controls about the use of roster information, using it only for the purposes of managing events and training. For Admin and Read-only training managers, it is controlled by password. Privacy notices are available site-wide for anonymous browsing, as well as explicitly on pages where participants sign up for events and training.

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

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:

Mitigation: