United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

System Name: Contaminated Site Clean-Up Information (CLU-IN)	
Preparer: Michael Adam	**Office: Office of Solid Waste and Emergency Response, Office of Land and Emergency Management**
Date: 11/01/2017	**Phone: 703-603-9915**
Reason for Submittal: New PIA_✔_ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition ☐ Implementation ☐	
Operation & Maintenance ☒ Rescindment/Decommissioned ☐	
Note: 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.

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 agreements permit and define the collection of information by the system in question?

Definition (why we have the systems, training) :

The need for 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?

Yes, this system was last authorized to operate on August 24, 2015. A new ATO package is being prepared for a FedRAMP Authorized Virtual Private Cloud instance, which includes a draft final ISSP from September 2017.

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.

N/A

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 publically and tangent/additional to the utility of the technical information.

This is N/A for the purposes of course registration.

2.4 Discuss how accuracy of the data is ensured.

The routine review of user-supplied information is limited to ensuring valid email address syntax through automated validation included with online forms. No other user-supplied information (for the purpose of course registration) is reviewed for accuracy.

Technical information (for information exchange) supplied is verified for technical relevance and applicability, authorship/contact information is not modified from the information from which time it was collected as a whole. That is, we do not modify final outputs to correct for moves or changes in the authorship information.

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 Uses of the Information

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

3.1 Describe how and why the system uses the information.

The primary uses of user-supplied 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.

3.2 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.*)

User-supplied business email addresses are used to retrieve information that is only delivered to the specified email address. Personal identifiers cannot be used to retrieve and display information directly within the user's browser.

3.3 If the system retrieves information by personal identifier, what types/elements of information about the user are being retrieved?

All user-supplied information, as well as webinar and class participation records for that individual are supplied to the individual email account provided by the user.

3.4 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information? N/A (we don't have a SORN)

3.5 Does the system use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how EPA plans to use such results.

No. We use anonymous tracking data in order to evaluate website usage. We do not analyze collected PII in this way.

3.6 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.

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

Privacy Risk:

Mitigation:

Section 4.0 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.

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

Registrants are provided with a privacy statement linked from the registration form notifying them that personally identifiable information is collected only if specifically and knowingly provided by the user, and any information collected is used only for the stated purpose. https://clu-in.org/conf/itrc/register/privacy.htm (partner example);

"Any information collected within the context of this registration form is used only for the expressed purpose of registering you for an online seminar. No personal information collected is sold or otherwise transferred to parties other than the U.S. Environmental Protection Agency or the Interstate Technology and Regulatory Council."

https://clu-in.org/conf/tio/register/privacy.htm (EPA example);

"Any information collected within the context of this registration form is used only for the expressed purpose of registering you for an online seminar. No personal information collected is sold or otherwise transferred to parties other than the U.S. Environmental Protection Agency."

https://trainex.org/usenotice.cfm

"Where identifying information is asked of you (such as to respond to an information request) that information is provided voluntarily by you. It is used only for the stated

purpose and is not made available for other purposes. By providing this information voluntarily, you are consenting to its collection for the stated purpose."

See also:

https://clu-in.org/privacy/

https://clu-in.org/privacy/use.cfm

4.2 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?

Webinar users may contact CLU-IN technical support through the email address provided on the registration form if they wish to participate in a webinar without providing PII. This option is not available for classroom courses since most are held within federal facilities.

4.3 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:

Participants in events and course are unaware how their information is used and for what purpose(s).

Mitigation:

The notice(s) alerts participants that their information will be used for the stated purpose: registration of a public or gov internal technical course that is either delivered online on in-person. The System allows users to contact technical support on an individual basis to register alternatively.

Section 5.0 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.

5.1 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).

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

No.

5.3 Who *(internal and external parties)* will have access to the data/information in the system? If contractors, are the Federal Acquisition Regulations (FAR) clauses included in the contract (24.104 Contract clauses; 52.224-1 Privacy Act Notification; and 52.224-2 Privacy Act)?

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.
- 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, including clauses 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)

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

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.

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

Information is retained indefinitely to support webinar and class registrant transcripts. The system does not have an EPA Records Control Schedule. 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).

5.6 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

No.

5.7 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 with the stated purpose and mission of the system.

Privacy Risk: Records may be retained after their perceived use is no longer necessary, increasing the risk of unauthorized PII released.

Mitigation: The section of the System (Trainex and CLUIN) that retains the training records does so for the convenience of the participants and their supervisors (in some cases, short-term, as required) and is retained indefinitely to support webinar and class registrant transcripts. (or until directed otherwise)

Section 6.0 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.

6.1 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.

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.

6.2 Describe how the external sharing noted in 6.1 is compatible with the original purposes of collection in the SORN noted in 3.4.

N/A

6.3 Does the agreement place limitations on re-dissemination?

No.

6.4 Describe how the system maintains a record of any disclosures outside of the Agency.

Disclosures are filed by the EPA Task Order Managers responsible for the CLU-IN system. Information is disclosed for course management only and is a known disclosure by the users/participants before they provide their professional/business contact information. Sharing this information with course managers is a necessary business function and records are not stored or maintained.

6.5 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?

Rosters are shared without formal agreements for the purposes of each organization's own courses (that is, one org's course registration information is not shared if it is not involved in the course). Anonymous tracking data may be shared for demographic purposes, but this does not contain PII. 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.

6.6 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?

The sharing of this information is for business purposes to allow other organizations to leverage our platform for like-mission training; and for course managers/supervisors to verify registration and course management. We do not share this information over the System publically. The risk is that business contact information or knowledge that a specific individual may be registered for a classroom or online technical course in environmental site cleanup could become public.

Privacy Risk: Partners may disclose course roster PII to the public. The risk is that business contact information or knowledge that a specific individual may be registered for a classroom or online technical course in environmental site cleanup could become public.

Mitigation:

Sharing is limited to management of courses. The sharing of this information is for business purposes to allow other organizations to leverage our platform for like-mission training; and for course managers/supervisors to verify registration and course management. We do not share this information over the System publically. Participants only have access through the System to this via an email system, for EPA employees, this system would be subject to the Agency's infrastructure security controls.

Section 7.0 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.

7.1 What are the procedures that allow individuals to access their information?

Users may access and review their information through email requests to the EPA Task Order Managers responsible for the CLU-IN system.

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

Users may submit any corrections to their information through email requests to the EPA Task Order Managers responsible for the CLU-IN system. These corrections are then implemented by contractor support staff from EMS, Inc.

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

The system notifies individuals about the procedures for correcting their information in response to email inquiries to the EPA Task Order Managers responsible for the CLU-IN system.

7.4 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: Participants cannot make convenient changes to their information or have it removed from the system.

Mitigation: Users may submit any corrections to their information through email requests to the EPA Task Order Managers responsible for the CLU-IN system. These corrections are then implemented by contractor support staff from EMS, Inc. Users/Participants do not need to utilize the Privacy Act/FOIA.

Section 8.0 Auditing and Accountability

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

8.1 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 publically, 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.

8.2 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).

8.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

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