United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 04/2019)
(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official
http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf. If you need further assistance, contact your LPO.

System Name: Financial Assurance Compliance Tracking Tool (FACTT)	
Preparer: Richard Hackley	**Office: EPA Region 5 / OMS / Comptroller Branch**
Date: 11/27/2019	**Phone: (312) 886-9144**
Reason for Submittal: New PIA_X___ Revised PIA____ Annual Review____ Rescindment ____	
This system is in the following life cycle stage(s):	
Definition ☐ Development/Acquisition X 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:

FACTT is a Financial Assurance Compliance Instrument tracking web-based application. It provides financial analysts with check lists and calculators when reviewing instruments so that EPA does not accept financial instruments that do not meet EPA financial instrument compliance criteria. It is not the system of record for Financial Assurance compliance. For Resource Conservation and Recovery Act (RCRA) facilities, the RCRA system is the official system of record. For Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) site cleanups, Superfund Enterprise Management System (SEMS) is the official system of record. FACTT compliments these systems, so that FACTT users are assured that the financial instruments are compliant before entering, or updating the Financial Assurance (FA) data in those Enterprise systems.

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?

EPA has promulgated regulations under the Toxic Substances Control Act[1] Section 6 of TSCA, 15 U.S.C.§ 2605 regarding the storage and disposal of Polychlorinated Biphenyls (PCBs) at 40 C.F.R.Part 761. Those regulations either require or provide authority for requiring financial assurance. Commercial storers of PCB waste are required to have closure plans and financial assurance for closure of their facility which complies with the RCRA regulations for closure instruments at 40 C.F.R 264.143. See 40 C.F.R. § 761.65 (g). In addition, EPA may require a financial assurance for a PCB disposal facility requiring an approval when it concludes that such a requirement is necessary to ensure that the operation of the facility does not present an unreasonable risk of injury to health or the environment from PCBs. See 40 C.F.R. 761.70 (d) (4) for incinerator approvals and 40 C.F.R. § 761.75 (c) (3) (ii) for chemical waste landfills. Those financial assurances for operation of an incinerator or landfill likely would rely on the types of mechanisms provided under RCRA.

EPA has promulgated regulations establishing permit conditions for certain underground injection wells pursuant to the Safe Drinking Water Act.[2] 40 C.F.R. §144.52 requires a permittee to demonstrate and maintain financial responsibility to close, plug, and abandon the underground operation through an approved plan and a bond or other financial assurance mechanism deemed adequate by the Regional Administrator. In addition, since 1984, new Class I- hazardous waste injection wells must provide EPA financial assurance for plugging and abandonment with instruments meeting requirements that are substantially the same as those for closure of RCRA hazardous waste facilities. See 40 C.F.R. Part 144, Subpart F.

EPA promulgated regulations on December 10, 2010 for a new class of Safe Drinking Water Act injection wells (Class VI). Those are wells used for the injection and sequestration of carbon dioxide. See 75 Fed. Reg. 77291, 40 C.F.R. Part 146, Subpart H. Those regulations also use the instruments allowed by the RCRA regulations. In order to assure that there are sufficient resources to provide for any needed corrective action, post injection site care and closure, are properly plugged and abandoned, emergency and remedial response work, and sufficient to address the contamination of underground resources. See 40 C.F.R § 146.85.

EPA has often required a demonstration of financial assurance in consent decrees and administrative orders providing for response action work under CERCLA. These requirements are imposed through injunctive and settlement authorities rather than regulations. Those financial assurance instruments likely compose the majority of the financial assurance instruments received by EPA.

As Responsible Parties submit financial assurance instruments to for reviews authorized FACTT enters relevant business contract name, business organization name, business organization address and business telephone number into the FACTT application.

[1] Section 6 of TSCA, 15 U.S.C.§ 2605.
[2] 42 U.S.C §300(f) et. seq.

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 (ATO)? When does the ATO expire?

Yes, FACTT SSP is developed and system has undergone initial assessment. Region 5 is actively working with the Office of Information Security and Privacy (OISP) ATO review team to resolve findings and address POAMS. The Initial ATO Decision date is targeted for the end of February 2020. ATO expiration date is not applicable. Phase 3 responses (including the PIA) are due by COB, 1/2/2020.

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?

Yes, AWS US East-West, has been granted a Joint Authorization Board Provisional Authority-To- Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for moderate impact level. The AWS East-West is FEDRAMP approved.

What type of service (PaaS, IaaS, SaaS, etc.) will the CSP provide?

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).

Financial analysts collect, process and store business information such as Business Name, Business Address, Business Telephone Number, and Business Email. It provides financial analysts with check lists and calculators when reviewing instruments so that EPA does not accept financial instruments that do not meet EPA financial instrument compliance criteria.

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

Responsible Parties submit financial instruments to EPA financials analysts for sufficiency review processes. Use of FACTT for instrument review is currently optional to the given Region or State.

For CERCLA, documents frequently submitted from the Regional Counsel for financial reviews include CERCLA Settlement Documents (Unilateral Administrative Orders, Administrative Orders on Consent and Consent decrees) which set the initial level of Financial Assurance required to be maintained. The level of financial assurance required for RCRA, (Closure/Post Closure and Corrective actions) is determined by the EPA RCRA facility Project Managers and provided to the financial analyst, usually via email.

Financial instruments are submitted via postal mail by CERCLA and RCRA Responsible Parties for review by the financial analyst. While R5 prefers financial instruments be submitted directly to the financial analyst via postal mail, sometimes they are sent to the Project Managers and are then forwarded to the financial analyst.

Third party Financial Instruments include General Liability Insurance polies, Insurance Policies payable directly to EPA, Trust and Escrow Account Statements, and Letters of Credit.

Where RPs maintain they have a solid financial base, they can submit Financial Statements or Corporate Guarantees for review. If a company passes the financial test, it would not be required to purchase Third Party coverage.

Pertinent source information is obtained from the submitted documents and input into the FACTT in order to determine if the documents meet EPA requirements.

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. Responsible Parties are required to submit financial instruments directly to EPA.

2.4 Discuss how accuracy of the data is ensured.

FACTT does not import data extracts from other systems. As discussed in 2.1 data is manually entered from the source documents submitted to the financial analyst. The Financial Analyst has the ability to reconcile the sources documents to the data entry screens and can run reports to verify data accuracy. The financial analyst shares the results of the review with the RCRA and CERCLA FA points of contact (POCs), who then enter the finalized information into RCRAInfo and SEMS. The RCRA and CERCLA staff perform a cursory review of the FA analysis before they enter the FA into those systems.

There is currently an ongoing programming requirement to automate a reconciliation of FA Data between FACTT and RCRAInfo and FACTT and SEMS which are the existing recognized SORNS. This will help mitigate issues of inconsistency between all of the systems. Current SEMS and RCRAInfo system reporting structures provide FA reports that can be extracted to an Excel file and the Excel FA can be compared offline to FACTT to

ensure data consistency between FACTT and the SORNs.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

There is risk of collecting incorrect information or more information than is required.

Mitigation: Data is collected directly from documents submitted EPA Regional Counsel and Responsible parties and FACTT users are obliged to review the accuracy of all data entered into FACTT.

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, the system offers several mechanisms to secure to data access control rules, password authentication and SSL. Non-privileged users are prevented from executing privileged function and mitigates the risk that unauthorized individuals process many gain unnecessary access to information or privileges. Restricting non-privileged users also prevents an attacker who has gained access to a non-privileged account, from elevating privileges, creating accounts, and performing system checks and maintenance. Users will utilize a username/password combination factor 1 and a One-Time password (OTP) for factor 2 for system access.

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

Access control is documented in the User Access Control Plan.

The system uses role-based access authorization. Logical access controls are employed to permit only authorized access to the system and restrict users to authorized transactions, function and data. These automated controls ensure that only authorized individual access to FACTT, users are assigned an appropriate level of privilege and that they are individually accountable for their actions. These controls support the separation of duties principle.

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

Yes – The FACTT application protects confidentiality and integrity of data, at rest, through a number of controls, including restricting read-only or read-write access to data to users whose roles permit such actions, limiting permission access rights consistent with least-privilege model. FACTT offers five user types (Group Admin, Group User, Group Visitor, Admin Visitor and Visitor) each of which has a different set of read/write permissions outlined in the FACTT User Manual

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 to FACTT is strictly limited to a very small group of EPA and State Agency employees with a bonafide business need to access the FACTT Financial Assurance data. Access is role-based based upon level of business need.

EPA FACTT Contractors are not users of the FACTT in the sense that they do not enter data nor run reports for the actual FACTT Users. The Contractors do have access to the data and have created User Test accounts in the Development version of FACTT that are used for quality assurance activities. We do have Contractors that provide development and hosting support activities under GSA Contract GS-10F-0061N. The following FAR clauses are incorporated into that GSA Contract:

- 52.204-21 Basic Safeguarding of Covered Contractor Information Systems (June 2016);
- 52.224-1 Privacy Act Notification (April 1984);
- 52.224-2 Privacy Act (April 1984);
- 52.224-3 Privacy Training (Jan 2017)
- 52.237-2 Protection of Government Buildings, Equipment and Vegetation (April 1984);
- 52.239-1 Privacy or Security Safeguards (August 1996);
- 52.227-14 Rights in Data- General (May 2014)

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.

As FACTT is not the System of Record for Financial Assurance.

Since FACTT stores financial assurance data related to the EPA RCRA and CERCLA Programs, the following record schedules apply to FACT:

CERCLA Superfund Site Specific Enforcement Actions are covered under EPA Records Schedule 0025. The electronic records cannot be disposed in FACTT until 30 years after the later of the date of completion of the cleanup up or cessation of enforcement actions related to the cleanup. FACTT has the ability to show a site or facility's need to for Financial Assurance as no longer required, so we could use that as a target date for archiving data to the National Archives.

Disposition Instructions:

Item a: No legal action required and routine legal action cases

- Disposable
- Close inactive records upon settlement or closing of case.
- Destroy 30 years after file closure.

Item b(1): Landmark cases - Nonelectronic

- Permanent
- Close inactive records upon settlement or closing of case.
- Transfer to the National Archives 30 years after file closure.

Item b(2): Landmark cases - Electronic

- Permanent
- Close inactive records upon settlement or closing of case.
- Transfer to the National Archives 5 years after file closure, with any related documentation and external finding aids, as specified in 36 CFR 1235.44-1235.50 or standards applicable at the time.

Item b(3): Landmark cases - Electronic copy of records transferred to the National Archives

- Disposable
- Close file upon transfer to the National Archives.
- Delete after electronic record copy is successfully transferred to the National Archives.

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:

- Records may be retained longer than described in the records control schedule.
- Unauthorized individuals gaining access to PII.

Mitigation:

- FACTT complies with the records control schedule.
- Unique ID and dual-factor authentication to FACTT is enforced.

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.

Not applicable. FACTT does not share PII data externally.

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

Not applicable. FACTT does not share PII data externally.

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?

Not applicable. FACTT does not share PII data externally.

4.4 Does the agreement place limitations on re-dissemination?

Not applicable. FACTT does not share PII data externally.

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:

There's no risk. FACTT does not share PII data externally.

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 in accordance with stated practices in this PIA (Section 6.1)?

Access to the FACTT is restricted to those with valid ongoing business needs Users work to ensure all required information is collected accurately and ensure that the information is used for the sole purpose for which it is collected. There are numerous controls in place to ensure data integrity and to prevent unauthorized uses. Access is controlled by users' roles, each assigned role gives access only to the data users need within that role to perform their job. All

the data is encrypted in AWS S3. FACTT Rules of Behavior outlines data is for solely for business purposes.

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

Privacy training is included as part of the mandatory Annual Information Security and Privacy Awareness training. This includes definition of what constitutes PII, safeguards and best practices to handle PII.

All users are required to read and acknowledge the FACTT rules of behavior that governs the appropriate use of information system.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: Improperly implemented auditing and accountability safeguards could allow authorized user to access their authority/use of the data for unofficial/unauthorized purposes.

Mitigation: Concurrent login access is not permitted. Only one authorized user can login and make changes to a given record at a given time. FACTT keeps a record of all changes to the system data via its change control 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.

FACTT is a Financial Assurance Compliance Instrument tracking web-based application. It provides financial analysts with check lists and calculators when reviewing financial instruments so that EPA does not accept financial instruments that do not meet EPA financial instrument compliance criteria.

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.*)

Information can only be retrieved by Company Name, or a combination of RCRA/CERCLA site/facility names or ID numbers.

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:

Individuals authorized to access PII could exceed their authority and use the data or unofficial/unauthorized.

Mitigation:

PII stored in FACTT is only viewable by specific personnel with a need to know the information, i.e., employees who require access to perform their job functions and individuals are required to sign the FACTT rules of behavior to use the data for solely business porpoises.

FACTT National and Regional Coordinators strictly manage access control and limit the use and access of all data for the purpose for which is was collected. Only data that is necessary for the purpose for which the system was designed is collected. No sensitive PII is collected.

*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: