United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev 8/2026 – 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://work.epa.gov/privacy/senior-privacy-officials-staff-lpos

System Name: FTTA Database *previously Federal Technology Transfer Act (FTTA) and Inventory for Patent Inventions (IfPI)		**System Owner:** Maggie Lavay	
Preparer: Meghan Sheehan		**Office:** AO/OASES/SED/SPB	
Date: 08/24/2026		**Phone:** 513-569-7434	
Reason for Submittal:			
New: ☐	Revised: ☐	Annual Review: X	Rescindment: ☐
System Lifecycle Stage(s):			
Definition: ☐	Development/Acquisition: ☐	Implementation: ☐	
Operation & Maintenance: X	Rescindment/Decommission: ☐		

Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).

The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).

Provide a general description/overview and purpose of the system:

The FTTA Database system is the embodiment of the Federal Technology Transfer Act (FTTA) and Inventory for Patent Inventions (IfPI) systems in a shared database system. The purpose of the system is to provide the opportunity for knowledge and expertise within the Agency to be shared with outside entities through collaborative agreements and licensing. Records are maintained for the purpose of documenting inventions made under EPA sponsorship, including filing patent applications, determining

rights to inventions, licensing inventions, and ascertaining inventorship and priority of invention.

The system houses FTTA data from mechanisms: Cooperative Research and Development Agreements (CRADAs), Materials CRADA (MCRADAs), Materials Transfer Agreement (MTAs), and Non-Disclosure Agreement (NDAs). For each agreement, the system tracks general information for the partner and EPA, including a description of the project, potential products, associations, budgets. The system also tracks the status and workflows of each agreement.

The system also houses FTTA data from Employee Reports of Invention (EROI) and tracks Patent License Agreement and Patent Application/Issued Patent information. The License information is identical to how we track our FTTA agreements. The Patent information includes information listing inventors and relative information regarding new inventions.

This database system resides on the BAP platform.

Section 1. Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

15 USC 3710, Utilization of Federal Technology.

15 U.S.C. 3710a. Cooperative Research and Development Agreements.

35 U.S.C. Ch. 18 (Patent Rights in Inventions Made with Federal Assistance), 37 CFR parts 401, 404, and 501.

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have, or will the system be issued an Authorization-to-Operate? When does the ATO expire?

The FTTA Database is housed in the Salesforce platform authorized by OFA. The ATO expires on June 26, 2027. No data in the FTTA database is accessible without an EPA email address. Salesforce has its own security plan which our system falls under.

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, the data will be stored in the Salesforce EPA cloud. The Salesforce cloud has an ATO expiring on June 26, 2027.

Section 2. Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Agreements & Licenses: Name, business email address, business telephone number, work address.

Patents: Invention reports (name and address), patent applications (name and address) until application is published, patents (name, city, and state), patent assignments (name), procurement requests (name & address), and other documents relevant to inventions.

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

FTTA Contacts fill out downloadable forms and then email them to EPA email address. The email is encrypted.

Invention report submitters and their supervisors; other persons with knowledge of the invention or expertise in the particular area of the invention; EPA Patent Counsel; EPA contractors who have searched the invention, prepared a patent application on the invention and/or otherwise performed work relating to a patent application; and the United States and foreign patent offices.

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.

Staff keeps data up to date by contacting partners and other contributors. Data is also maintained by the assigned 'Owner' and OGC attorney.

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:

A potential to access a business partner's personal email or phone number, if they do not have a functional business number.

Mitigation:

When information is considered sensitive, we do not enter this content into our database.

Section 3. Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place, why have they been omitted?

Yes – Salesforce controls access. The BAP uses all the extensive access controls of the Salesforce Lightning Platform, including user and group profiles, permission sets, object-level permissions, record-level permissions, field-level permissions, and other fine-grained access controls. Detailed information is available at http://login.salesforce.com/help/pdfs/en/salesforce_security_impl_guide.pdf. Core users have written access; Lab contacts have view only access.

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

We created user guides to help identify user access. Generally, core users include FTTA, OGC staff that work on the FTTA team. The Salesforce admins also provide level of access based on guidance from the FTTA and OGC staff that work on the FTTA team. Access is determined through assignment of Salesforce Lightning Platform permission sets.

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

Users have different roles/responsibilities, and the Salesforce admins provide different levels of access as needed.

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?

Only internal access. No contractor will have access to FTTA Database.

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.

This FTTA Database system uses SORN EPA-38 and are maintained according to EPA Records Control Schedule 1035. The records are permanent, are closed when the file/activity is completed, and are transferred to NARA 15 years after file closure.

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:

Potential access to partner or inventor contact information may occur; potential access to budget information for Cooperative Research and Development Agreements; potential access to confidential information used in the creation of patent filings.

Mitigation:

Only personnel with an EPA email address may access the database system; database system access is limited to need-to-know personnel; sensitive information is omitted from the database.

Section 4. Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local governments, 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. Information is not shared externally.

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

N/A

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?

N/A

4.4 Does the agreement place limitations on re-dissemination?

N/A

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. Information is not externally shared.

Mitigation:

None.

Section 5. Auditing and Accountability

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

5.1 How does the system ensure that the information is used as stated in Section 6.1?

The system only allows admin users to have access to the complete data needed to send the reports to congress. The FTTA database has user timestamp feature that indicates who modified the system and at what time it was modified. Rules of Behavior that is required and training is provided to all required personnel.

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

None other than the annually required Information Security and Privacy Awareness Training. First time users are also trained on FTTA system.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

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

Privacy Risk:

The risk exists that applications being hosted on the BAP could have inadequate privacy controls at the application level, not taking sufficient advantage of the controls provided by the platform. Auditing may expose risks. Application owners are accountable to mitigate risks.

Mitigation:

OMS will manage all risks associated with Auditing and accountability. In conducting Conceptual Review, Design Review, and Production Readiness Review for an application, the BAP Program Office reinforces that the application must have sufficient privacy auditing and accountability controls in place.

Section 6. Uses of the Information

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

6.1 Describe how and why the system uses the information

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

Information is needed to maintain congressionally mandated program under FTTA, to get technologies transferred from Federal laboratories to the marketplace through partnerships and collaborations. This is tracked via the database to show what EPA has done to influence the marketplace.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes: ☒ No: ☐ If yes, what identifier(s) will be used.

A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e. any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.

The system also includes a search box where a user can search by File number, case number, or business name.

The data will be retrieved by the name of the company or automatically generated number generated by Salesforce.

For information related to Inventory for Patent Invention, users retrieve data by inventor's name, case identification number, and patent application number or patent number. This system merges with the FTTA and IfPI system. The IfPI database retrieve information by name. This system will use SORN EPA-38. EPA-38 will be modified to change the name, location, ownership as well as to update the data elements to include data elements in the FTTA.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

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

There are controls in place to protect PII in the system.

ORD FTTA Core team has elevated privileges to access system, approve workflow, and ad-hoc reporting dashboard. OGC team has same but cannot delete.

Lab Contacts - have view-only privileges but are able to use communications features – upload files, email and task features.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

There is a low risk associated to data misuse.

Mitigation:

The FTTA database has user timestamp feature that indicates who modified the system and at what time it was modified. Privacy risk mitigation is a function of both the source systems and the BAP security plan, which describes in detail the controls in place for the BAP. For example, the Business Automation Platform requires login using Agency LAN ID and password in accordance with FISMA Moderate level controls specified in the BAP security plan.

If no SORN is required, STOP HERE.

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

Section 7. Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

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

Any individual who wants to know whether this system of records contains a record about him or her, should make a written request to the Attn: Agency Privacy Officer, MC 2831T, 1200 Pennsylvania Ave., NW., Washington, D.C. 20460, privacy@epa.gov.

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?

By filling out and signing the EROIs, the EPA employees consent to the collection and sharing of their information in this system.

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:

Low risk of inadequate notice.

Mitigation:

Adequate notice is provided prior to information collection. Salesforce Platform has controls in place to prevent access to unauthorized users.

Section 8. Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals fill out the information themselves. So, we accept it at face value. They have no access once they have filled out the information.

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

They contact OGC or FTTA staff to correct inaccuracies if they see them.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and Freedom of Information Act (FOIA).

Privacy Risk:

There is a procedure in place for users to correct inaccuracy.

Mitigation:

There is a procedure in place for users to correct inaccuracy.

I attest as the Agency Privacy Officer that **FTTA Database** Privacy Impact Assessment (PIA) has been reviewed. The privacy implications have been adequately identified with appropriate mitigation statements included for implementation in the development or use of information technology systems.

Respectfully,

ROBERT KELLY

Digitally signed by ROBERT KELLY
Date: 2026.09.03 10:28:56 -04'00'

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