

# PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020)

(All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official. *All entries must be Times New Roman, 12pt, and start on the next line.* If you need further assistance, contact your LPO. A listing of the LPOs can be found here:

[https://usepa.sharepoint.com/:w:/r/sites/oei\\_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx](https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO%20Roster.docx)

<b>System Name: Federal Technology Transfer Act (FTTA) and Inventory for Patent Inventions (IfPI)</b>	<b>System Owner: Kathleen Graham</b>
<b>Preparer: Ronny Escobar</b>	<b>Office: ORD/ORM/EMD/PFTTB</b>
<b>Date: 8/3/2021</b>	<b>Phone: (202) 564-4668</b>
<b>Reason for Submittal: New PIA___ Revised PIA__X__ Annual Review___ Rescindment ___</b>	
<b>This system is in the following life cycle stage(s):</b>	
Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input type="checkbox"/>	
Operation & Maintenance <input checked="" type="checkbox"/> Rescindment/Decommissioned <input type="checkbox"/>	
<b>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 <u>OMB Circular A-130, Appendix 1, Section (c) (1) (a-f).</u></b>	
<b>The PIA must describe the risk associated with that action. For assistance in applying privacy risk, see <u>OMB Circular No. A-123, Section VII (A) (pgs. 44-45).</u></b>	

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

Federal Technology Transfer Act (FTTA) and Inventory for Patent Inventions (IfPI) Program provides the opportunity for the knowledge and expertise within the Agency to be shared with outside entities through collaborative agreements and licensing. The system houses FTTA 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. We have a description of the project, potential products, associations, budgets. The system also tracks the status and workflows of each agreement.

IfPI contains Employee Reports of Invention (EROI) database. This database which tracks License and Patent information. The License information is identical to how we track our FTTA agreements. The Patent

information includes our inventors and relative information regarding new inventions. This is contained as attachments of EROIs in the database. This application will reside on the BAP platform.

This system merges the FTTA and IfPI system. The IfPI database retrieves 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.

## **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?**

Congressionally mandated, EPA Agency-wide program facilitated by ORD

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?**

Yes. ATO expires on September 30, 2021. Salesforce platform authorized by OMS/OEI for agency use. Not 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. There was a paper process leaned by the ORD Management Council approval.

### **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 September 30, 2021

## **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).**

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 3.0 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 – 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](http://login.salesforce.com/help/pdfs/en/salesforce_security_impl_guide.pdf). Core users have write 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 level 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.

**Privacy Risk:**

There is a low risk of over keeping the data longer than needed.

**Mitigation:**

Will follow the EPA records Schedule 1003b and adhere to all requirements.

## **Section 4.0 Information Sharing**

*The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state, and local government, and third-party private sector entities.*

**4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.**

No. 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 5.0 Auditing and Accountability**

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

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

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**

#### **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 6.0 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.**

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 X 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 has list views that can be filtered, depending on user preference, to present data. 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 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?**

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

ORD FTTA Core team has elevated privileges to access system, approve workflow, 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 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.**

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](mailto: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 in adequate notice.

#### **Mitigation:**

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

## **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?**

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 any inaccuracies.

### **8.3 Privacy Impact Analysis: Related to Redress**

*Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.*

#### **Privacy Risk:**

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

#### **Mitigation:**

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