

# 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.*

[http://intranet.epa.gov/privacy/pdf/lpo\\_roster.pdf](http://intranet.epa.gov/privacy/pdf/lpo_roster.pdf). If you need further assistance, contact your LPO.

|  |                              |
|--|------------------------------|
| <b>System Name:</b> Paper Asset Tracking Tool (PATT)   |                              |
| <b>Preparer:</b> Shahjahan Khan/Andrew Yuen  | <b>Office:</b> OMS/OEIP/ERMD |
| <b>Date:</b> 5/01/20   | <b>Phone:</b> 202-566-1226   |
| <b>Reason for Submittal:</b> New PIA <input checked="" type="checkbox"/> Revised PIA <input type="checkbox"/> Annual Review <input type="checkbox"/> Rescindment <input type="checkbox"/>  |                              |
| <b>This system is in the following life cycle stage(s):</b>  |                              |
| Definition <input type="checkbox"/> Development/Acquisition <input type="checkbox"/> Implementation <input checked="" type="checkbox"/>  |                              |
| Operation & Maintenance <input 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><a href="#">OMB Circular No. A-123, Section VII (A) (pgs. 44-45)</a></u>.</b>  |                              |

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

The United States Environmental Protection Agency’s Enterprise Records Management Division (ERMD) within the Office of Environmental Information’s (OEI) Office of Enterprise Information Programs (OEIP) provides leadership and direction in managing records that support EPA’s mission. ERMD, in collaboration with other Agency records management experts, is engaged in development, operation and maintenance of the Enterprise Content Management System (ECMS) Paper Asset Tracking Tool (PATT) so as to further enhance Records Management capabilities of EPA through digitization.

The main purpose of ECMS PATT is to assist with record digitization initiative by implementing a robust asset management mechanism because that will be critical to the ongoing success of the centralized records digitization centers of ERMD. This asset management tool (PATT) will allow custodians of paper records to submit new digitization request. Once these requests are submitted, the records custodian will be able to

track the status of the request from receipt to digitization to storage and eventual destruction. The asset management tool will allow digitization center managers to prioritize and assign digitization tasks to scanner operators. In addition, the asset management tool PATT will have the capability to send digitized records directly to ECMS where they will ultimately reside.

## **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?**

- Title III of the E-Government Act of 2002, Federal Information Security Management Act (FISMA) 44 U.S.C 3541 et seq
- The Privacy Act of 1974, PL 93-579, as amended 5 U.S.C 552a
- The Freedom of Information Act, PL 93-502 5 U.S.C 552
- The Federal Managers' Financial Integrity Act (FMFIA), PL 97-255
- OMB Circular A-130, *Management of Federal Information Resources*
- OMB Circular A-123 Revised, *Management's Responsibility for Internal Control*, December 2004
- OMB Circular A-127, *Financial Management Systems*, July 23, 1993
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*
- NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*

### **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, PATT has a Security Plan.

Currently PATT is seeking an ATT as it is in the Implementation Stage and has not gone live as of 5/01/20.

### **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?**

The PATT Tool is not a cloud-based application and does not store data in the cloud.

## **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 PATT Tool collect the following data elements:-

- Category
  - Site Specific
  - Non-Site Specific
- Customer Goal/Objective for Scanning Project
- Description
- Additional Information
- Index Level
  - Box Level
  - Folder Level
- Custodian
- Shipping Tracking Number
- Number of Boxes
- Lon(s)
- Date
- Record Schedule
- Sensitivity (CUI, Confidential Business Information)
- Accession Number?
- Box list document (csv)
- Box contains PII?
  - Yes/No
- Box contains PHI?
  - Yes/No
- Box contains CUI?
  - Yes/No

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

The Records Liaison Officer (RLO) will provide metadata information to the system describing the paper records that need to be digitized and this information will be collected

using an online form through the application.

**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.**

Accuracy of the data is ensured through a combination of system validation and review of the digitization request by the RLO. In addition, the digitization staff at the receiving digitization facility will review each request to ensure accuracy of the data.

**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 are no privacy risks for the specific data elements being collected by the system excepting low risk posed by internal users performing hostile acts. The PATT Tools does not have a public interface, so there would be no exposure to public release of the digitized data. There is a specific authorization required to use the PATT Tool which is controlled by the ECMS System Owner.

**Mitigation:**

PATT does not provide public access to paper or digitized data that it collects.

RLOs or digitization liaisons who are Agency employees approved by ECMS management – in addition to digitization staff, will be the only individuals allowed to access the PATT.

However, there may be a risk of misuse of the data which resides in the system/PATT temporarily.

Above risk will be mitigated by properly monitoring data usage (periodically review/update approved procedures for data-handling if needed) and by following controls:-

- User group access controls (only specific users can have access to data which may temporarily remain in the system)
- Appropriate Audit logs

## **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, the PATT tool is for internal use only.

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

No external sharing is done with the PATT tool.

**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?**

The PATT tool does not have an MOU/ISA with any other system.

**4.4 Does the agreement place limitations on re-dissemination?**

The PATT tool does not have an agreement with any external systems.

**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?*

The PATT is a tool designed for one specific purpose – to digitize forms. This tool does not interface with any external systems, and it does not have a public or generalized user interface. It is not open to Agency employee’s unless granted access by the System Owner.

**Privacy Risk:**

None. The PATT tool does not share information.

**Mitigation:**

None. Specialized access was built into the business process of digitalization to limit access to the Tool to a very, very select group.

## **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?

All transactions (for tracking paper assets as well as corresponding digitized records) are tracked within PATT through auditable events. The system does not alter the original content or time ordering of audit records. The system handles audit reduction and report generation capability by auditing functions within the database. The database creates customized reports based on the audit events in the system. These audit log are reviewed to ensure that information is used in accordance with stated practices.

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

Only EPA employees and approved contractors may request access to this system, which means they have completed and passed Information Security and Privacy Awareness Training.

### 5.3 Privacy Impact Analysis: Related to Auditing and Accountability

#### Privacy Risk:

Audit logs could be inadvertently lost.

#### Mitigation:

Server audit logs are kept for 90 days, some of that time on the instance and some of the time archived on a separate instance. Anything older than 90 days is deleted daily. In general they are on the DB server for about 24 hours then moved to the backup appliance. Audit records generated today would stay on the database for the rest of the day, then be moved to the separate database and kept for 90 days. The last backup of the separate database would be kept for another 90 days. That adds up to approximately 180 days' retention, 170 days to allow for the usual "expected" unexpected.

Request history audit logs which are tied to an individual digitization request are kept indefinitely.

## 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.

PATT uses the information for tracking paper assets as well as corresponding digitized records. It allows custodians of paper records to submit new digitization request then track the status of the request from receipt to digitization to storage and eventual destruction. PATT will allow digitization center managers to prioritize and assign digitization tasks to scanner operators and will have the capability to send digitized records directly to ECMS where they will ultimately reside.

- 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.)*

We are using Request ID, Box level ID and folder file ID to retrieve information but those are not linkable to individuals

- 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.]*

.A thorough evaluation of information handled by this system and related procedures was conducted, and following technical controls are in place (so that privacy is not invaded):-

- User group access controls (only specific users can have access to data which may temporarily remain in the system)
- Appropriate Audit logs
- Monitoring of data usage (including periodic review/update of approved procedures for data-handling if needed)
- Utilization of API security tool (APIMAN) which manages security of the data going through API gateway.

#### **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:**

PATT users can misuse the information in violation of the approved procedures and instructions provided by EPA

##### **Mitigation:**

In addition to core controls per FISMA directive, following technical controls are in place for tracking any misuse:-

- Utilization of API security tool (APIMAN) which manages security of the data going through API gateway

- User group access controls - requirement of specific authorization for use of data deemed sensitive by EPA
- Restriction (per EPA instructions) on any public release of the data
- Appropriate Audit logs
- Monitoring of data usage (including periodic review/update of approved procedures for data-handling if needed).

Additionally, each user is required to Sign a Rules of Behavior document when gaining access to the PATT tool.

**\*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 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:**