Privacy Impact Assessment (PIA)

for the

Parking Tracking System

May 20, 2021

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Barbara Shawyer, Management Analyst
Contact Email: Barbara.Shawyer@ed.gov

System Owner

Name/Title: Lee Flowe, Director Shared Services Systems Support Division
Principal Office: Office of Finance and Operations

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Electronic Case Management Platform (ECAMP) was developed to support the Office of Finance and Operations strategy of streamlining information technology (IT) operations to better align with the U.S. Department of Education's (Department) goal of IT modernization, standardize the use of IT shared services, and reduce the overall cybersecurity footprint. The ECAMP system will combine separate case management systems or modules, each with separate small contracts with Tyler Technologies, Inc. (formerly MicroPact), a cloud service provider (CSP).

The Parking Tracking System (PATS) is a web-based application that is platform-independent of other user operating systems (e.g., iOS, Windows). PATS allows employees, contractors, and visitors to apply for subsidized parking at the various Department-occupied buildings in headquarters and the Kansas City, Missouri, regional office. The system also calculates a parking application score which is determined by a number of factors (distance from the parking garage, number of approved telework days, service computation date, carpool status, etc.) and ranks applications to determine who receives parking passes. All Department employee parking is accounted for in this system.

PATS is a case management module supported via a Software-as-a-Service (SaaS) platform, known as Entellitrak. Entellitrak is a configurable data tracking and management platform for case management (CM) and business process management (BPM). It provides pre-built, executable business process management system (BPMS) based configurations (process templates) focused on a particular process domain or a vertical industry sector and supports storing data in either an Oracle database or Microsoft structured query language (SQL) server database. PATS is accessed via a web-based interface, utilizing a role-based security and access model. The system provides administration and tracking information to Department.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected,

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined

used, maintained or shared.

The information contained in this system is used to: (1) provide standards for apportionment and assignment of parking spaces on property occupied by the Department in Washington, D.C., and Kansas City, MO, and (2) allocate and check parking spaces assigned to government vehicles, visitors, handicapped personnel, executive personnel, carpool and van pools, and others.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

New PIA
PATS migrated to the Entellitrak SaaS platform, so a new PIA is required.

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Federal Property and Administrative Services Act of 1949, as amended, 40 U.S.C. 101 et. seq., which allows for the Federal Government to manage Federal property and Federal Management Regulations (FMR), 41 CFR 102-74.305, which allows for Federal agencies to establish the rules under which Federal agencies may allow for parking on General Services Administration (GSA) property.

---

with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

Parking Application Tracking System (PATS) (18-05-01) System of Records Notice was last updated on February 16, 2018 (83 FR 7026, 7026-7029).

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Click here to enter text.

Records Management

If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

NARA Records Schedule 622 addresses records related to assigning and controlling parking areas and spaces. The records are temporary, cut off when permit is returned or expires. Destroy 3 years after cutoff. (N1-64-87-1)

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by Department. https://connected.ed.gov/om/Documents/SORN-Process.pdf

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

PATS collects first name, middle initial, last name, home address, work email address, work phone number, employment status, Department principal office, employee service computation date, and automobile information such as make, model, registration, state, and license plate number. For visitors, business justification is also collected.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The system collects only that information necessary to determine eligibility for parking and to administer the parking program.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

Federal employees wishing to use Department-controlled parking spaces provide their information on the parking permit application. Visitors requesting parking provide information directly to the Department Transportation Service Office.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

Federal employees log into the PATS website and directly enter required information on the parking permit application. Visitors email information directly to the Transportation Service Office.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

Applicant information is manually validated by the employee submitting the application at the time of parking permit issuance and periodically throughout each fiscal year. Manual validation by the employee submitting the application is required annually before they are issued their parking permit with signature confirming information accuracy. Applications are automatically ranked by PATS after the application period has closed. Visitors submit information directly. If visitors submit inaccurate information, they will not receive a response from the Transportation Service Office.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

Federal employee information is used to help determine an applicant's eligibility and ranking for subsidized parking in Department-occupied buildings. Information is also collected from individuals seeking visitor permits to determine eligibility for visitor permits.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Click here to enter text.

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☑ N/A

Click here to enter text.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☑ N/A

Click here to enter text.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

A Privacy Act statement is provided prior to applicants entering information into the system. Public notices are also provided through this PIA as well as a SORN.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

https://edcts.entellitrak.com/etk-ed-frp-prod/page.request.do

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Federal employees not wishing to provide PII can decline to provide the information at the time of application open season. They would then not be eligible to apply for parking. Visitors requesting parking can decline to provide the information. They would then not be eligible for visitor parking.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other Department principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

The PATS system rarely discloses PII to other Department Offices.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☑ N/A

The PII contained in PATS is rarely disclosed within the Department of Education and is only disclosed for the purposes of the administration of the program. For example, should there be a threat identified within a parking facility, information would be shared with the security office and other supporting offices.

External

5.4. Will the PII contained in the system be shared with external entities (e.g., another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

OFO does not ordinarily share data with external parties. PATS may disclose information contained in a record in this system of records under the routine uses listed in this system of records without the consent of the individual if the disclosure is compatible with a purpose for which the record was collected. These disclosures are made on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act of 1974, as amended (Privacy Act), under a computer matching agreement.

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

There are a number of routine uses of disclosure of the PII in the PATS system. All are currently accounted for within the PATS SORN.

5.6. What is the purpose for sharing the PII with the specified external entities?

☑ N/A

The organization shares information external to the Department under the routine uses identified within the SORN.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?

☐ N/A

Information is shared in a secure and electronic fashion with external parties.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

No

5.11. Does the project place limitation on re-disclosure?

☐ N/A

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

Yes

As the project does not regularly disclose information, PATS will ensure that there is a limitation on any re-disclosures as required.

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

Federal employees can access their information at any time through the PATS website. Visitors can also contact the Transportation Service Office directly.

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

Federal employees can correct inaccurate or erroneous information at any time through the PATS website. Additionally, individuals may provide the system manager with name, agency and office, and the location where Department parking is provided, as well as information that reasonably identifies the record and the information to be contested. Your request must meet the requirements of the regulations at 34 CFR 5b.5, including proof of identity.

6.3. How does the project notify individuals about the procedures for correcting their information?

The PATS webpage has a user guide, policies and procedures, and a participation form that provides information regarding use of the PATS system. The SORN and PIA also provide this information.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

PATS is hosted outside of the Department's network on FedRAMP-certified CSP, Tyler Federal. The system is provided as a SaaS and is required to complete routine testing of their environment to ensure the confidentially, integrity, and availability of the information in the system and services provided. The CSP enforces security controls over the physical facility where the system is located in adherence with FedRAMP standards. PATS utilizes role-based authentication to ensure only authorized users can access information, and they can only access the information needed to perform their duties. Authentication to the server is permitted only over secure, encrypted connections. A firewall is in place which allows only specific trusted connections to access the data. PATS has an ATO in place and complies with all National Institute of Standards and Technology (NIST) standards.

Physical safeguards for the data centers are detailed within the system security plan and are assessed as part of the FedRAMP assessment. Tyler Federal does not consume, process, or view the customers' data; no hard copies are made.

MicroPact/Tyler Federal does not access customer production applications without specific approval from the system owner (possibly for troubleshooting purposes). The customer manages application- level access and accounts. Multiple layers of cryptographic mechanisms are in place. There is role-based access control within the application.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

MicroPact/Tyler Federal performs monitoring, testing, and evaluation of their software. MicroPact/Tyler Federal is responsible for ensuring access controls are working as defined in the software.

- As a part of their continuous monitoring plan, MicroPact/Tyler Federal evaluates and tests a selection of controls internally on a scheduled basis.
- Assessments are conducted annually by MicroPact/Tyler Federal's third-party organization as part of FedRAMP continuous monitoring requirement; results are reported within the security assessment report. Additionally, MicroPact/Tyler Federal supports multiple customer assessments each year and evaluates those results.
- Security documentation is reviewed by the information system security officer (ISSO) and the information system owner (ISO) at least annually and updated as required by changes to the system, security posture, or security requirements.

The system production environment has multiple monitoring tools in place. Infrastructure logs are audited. Application-level audit logs can be run by the customer from the administrative module. MicroPact/Tyler Federal also has a continuous monitoring plan in place, which schedules the evaluation/testing of select controls internally.

There are a number of reviews conducted by the PATS administrator to ensure only authorized users are accessing system data.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

Any current Department employee has access to PATS and can utilize system to provide and submit a parking application, but they can only access their own information. Parking administrators are provided access by the system administrator and are only given access to information necessary to perform their specific duties. Parking administrator access is reviewed annually with access being deleted for any parking administrators that no longer have the need to access the information. The ISO also works directly with the Department's privacy office on privacy compliance documentation to ensure all information in this PIA is up to date and accurate.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data.

Privacy risks are mitigated with the controls discussed within this PIA. Additionally, if the information contained in the system were exposed, the risk of the harm to the individuals would be low due to the nature of the information collected. The system contains only the information needed to administer the system, with system users having access to information needed to perform their duties. Risks are additionally mitigated by restricting employee access to only their own information and restricting parking administrator access to only information needed to perform specific duties.