Template Version Number: 01-2021

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Office of Civil Rights ETK EEO and ETK RA

U.S. Department of Commerce Privacy Threshold Analysis

Office of the Secretary/[Entellitrak EEO and Entellitrak Reasonable Accommodation]

Unique Project Identifier: [Number – FISMA ID number, or alternate number or name of the system in how it is identified in your IT systems inventory, whether in CSAM or via internal tracking]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

EntelliTrak (ETK) EEO and EntelliTrak (ETK) Reasonable Accommodation (RA) are two commercial off the shelf web-based applications used to support the Office of Civil Rights (OCR) and bureau Equal Employment Opportunity (EEO) offices. This application will assist in the entry, management and reporting of data related to EEO complaints and requests for reasonable accommodation.

The information collected in ETK EEO and ETK RA is personally identifiable information (PII) and business identifiable information (BII) for law firms, unions, and others who represent the complainants and contractors.

Address the following elements:

a) Whether it is a general support system, major application, or other type of system

Major Application - Platform as a Service (PaaS)

b) System location

The MicroPact Product Suite of Web-based applications is currently hosted under a contract within MicroPact, Inc., facilities located at 107 Carpenter Drive, Suite 140, Sterling, Virginia, 20164.

c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

The MicroPact Product Suite is bound by Firewalls and is not interconnected and it does not exchange information with other systems.

d) The purpose that the system is designed to serve

Micro Pact Engineering's ETK EEO and ETK RA are enterprise level COTS (Commercial Off-The Shelf) products that provide all the functionality required to collect, track, manage, process, and report on information regarding EEO complaints cases (ETK EEO) and reasonable accommodation requests (ETK RA).

e) The way the system operates to achieve the purpose

ETK EEO is a web-based application that allows DOC's OCR staff and a limited number of Bureau EEO staff to track and manage EEO complaints. The EEO staff who are designated users will have exclusive access to ETK EEO to enter data needed to track EEO complaints and to ensure the Department meets regulatory requirements. EEO staff from DOC bureaus will have access that is limited to the complaint data from their bureau.

ETK RA is a web-based application that allows one set of users to submit and process their reasonable accommodation requests and for another set (the reasonable accommodation coordinators) to manage and track those requests.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

The information collected in ETK EEO is personally identifiable information (PII) and business identifiable information (BII) for law firms, unions, and others who represent the complainants and contractors. The PII maintained in ETK EEO also includes medical documentation that is submitted as part of a Report of Investigation of complaints based on disability and failure to accommodate.

The PII also maintained in ETK EEO could also include, race, national origin, dates of birth, and gender of the Complainant depending on the basis alleged in the complaint process. The PII maintained in ETK RA contains contact information for employees, their supervisors, and applicants who are requesting reasonable accommodation. Medical documentation that relates to the RA request will not be maintained in this system. The information collected in ETK RA includes basic information relating to reasonable accommodation requests. Medical documentation or detailed information about a person's medical condition is not collected.

g) Identify individuals who have access to information on the system

ETK EEO licenses are limited to EEO staff from the OCR, NOAA, Census, and NIST. Only OCR users, with the exception of term appointment employees, can see case information

across the department. License management is performed by administrators in the Office of Civil Rights. The total number of licenses for the first two years of the contract is 35, which includes 11 term appointment employees working Decennial cases. Once the Decennial operations cease, the number of licenses drops to 25 (excluding PTO) for the remaining three years of the contract. These employees would no longer have access to ETK EEO and their accounts would be disabled upon separation.

ETK RA users will include all DOC employees except for contractors and United States Patent and Trademark Office. Use of this automated system to request a reasonable accommodation is optional for DOC employees, but highly recommended for efficient tracking of their RA requests. RA requesters will only have access to the "Request Page" to input basic information about their reasonable accommodation request. This includes inputting their contact information, job title/series/pay plan/grade, supervisor's contact information, brief information about their functional limitations and type of accommodation needed.

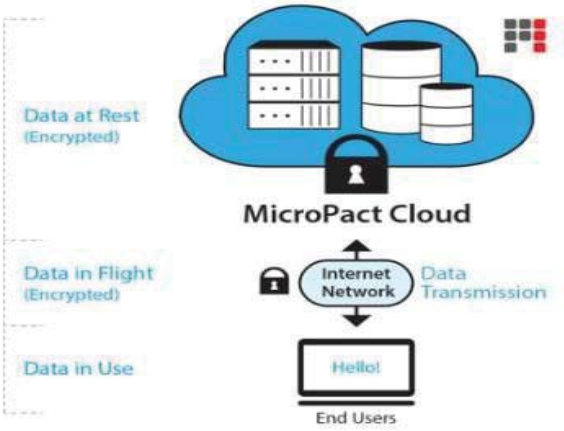
There are an additional 15 users that include: 13 Reasonable Accommodation Coordinators (RAC) from all Bureaus and the Office of the Secretary (OS) except USPTO; the Department's Disability Program Manager (DPM); and the Deputy Director OCR. The RAC users and the DPM will have access to the system to manage and track RA requests. They will have the ability to submit RA requests for users and job applicants who need reasonable accommodations, but do not have access to the system. Bureau RACs will only have access RA requests for employees within their bureaus. The DPM, Deputy Director, and OS RAC will also have Administrator rights that include resetting user passwords, managing user roles, and adding/removing RAC users accounts to the system.

h) How information in the system is retrieved by the user

ETK EEO records are typically pulled/retrieved by case number and/or last name. ETK RA records are pulled by last name or a tracking number which is created when the request is submitted.

i) How information is transmitted to and from the system

Please see the diagram below:



Data in flight is encrypted using TLS 1.2, ECDHE_RSA with P-256, and AES_256_GCM.

Data at Rest Encryption uses FIPS 140-2 validated AES 256-bit encryption on Intel® multi-core processors. Encryption keys are assigned per volume (vs. an entire disk or array) and stored separately from stored data.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify): Upgrading of iComplaints to ETK EEO and adding ETK Reasonable Accommodation as a new module but using the same platform, ETK.					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

X___ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

___ Yes. This is a new information system.

___ Yes. This is an existing information system for which an amended contract is needed.

___ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

____ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

____No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

_____Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____DOC employees
____Contractors working on behalf of DOC
____ Other Federal Government personnel
____Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

_____No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

X The criteria implied by one or more of the questions above **apply** to the ETK EEO and ETK RA system and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

___ The criteria implied by the questions above **do not apply** to the ETK EEO and ETK RA system and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Larry J. Beat Office: OCR Phone: (202) 821-6178 Email: lbeat@doc.gov Signature: LARRY BEAT Digitally signed by LARRY BEAT Date: 2022.02.16 15:07:01 -05'00' Date signed:	**Information Technology Security Officer** Name: Densmore Bartly Office: Office of the Chief Information Officer Phone: 202.482.3186 Email: dbartly@doc.gov Signature: DENSMORE BARTLY Digitally signed by DENSMORE BARTLY Date: 2022.02.16 17:30:39 -05'00' Date signed:
Privacy Act Officer Name: Tahira Murphy Office: Office of Privacy and Open Government Phone: 202.482.8075 Email: tmurphy2@doc.gov Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2022.02.23 17:19:08 -05'00' Date signed:	**Authorizing Official** Name: Lawrence W. Anderson Office: Office of the Chief Information Officer Phone: 202.482.2626 Email: landerson@doc.gov Signature: ROGER CLARK Digitally signed by ROGER CLARK Date: 2022.02.17 16:11:19 -05'00' Date signed:
Bureau Chief Privacy Officer Name: Maria Dumas Office: Office of Privacy and Open Government Phone: 202.482.5153 Email: mdumas@doc.gov Signature: Digitally signed by MARIA STANTON-DUMAS Date: 2022.02.23 17:58:04 -05'00' Date signed:	