Version Number: 01-2019

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the

Office of Civil Rights ETK EEO and ETK RA

Reviewed by: Maria D. Dumas, Bureau Chief Privacy Officer

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Jennifer Goode 02/22/2021

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
[O/S, OCFO/ASA, Office of Civil Rights, Entellitrak EEO and Entellitrak RA IT Systems]

Unique Project Identifier: OS-061

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

General Description:

EntelliTrak (ETK) EEO (formerly known as iComplaints) and EntelliTrack (ETK) Reasonable Accommodation (RA) are two commercial off the shelf web-based system used to support the Office of Civil Rights (OCR) and bureau Equal Employment Opportunity (EEO) offices. This applicaton will assist in the entry, management and reporting of data related to EEO complaints and requests for reasonable accommodation. iComplaints has been operational since November 4, 2010 and the platform is being upgraded to ETK EEO in 2020 because MicroPact is sunsetting iComplaints.

ETK is an additional module being purchased by the Department. 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.

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 any other systems.

d) The way the system operates to achieve the purpose

ETK EEO is a web-based application that allows DOC Office of Civil Rights 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 through the EEO process and to ensure the Department meets regulatory EEO staff from DOC bureaus will have access that is limited to the complaint data from their particular bureau.

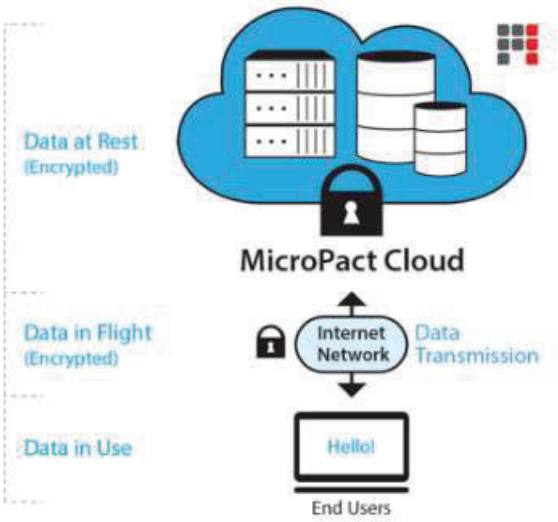
ETK RA is a web-based application that allows one set of users to submit and process their reasonable accommodation requests and for another set (the reasonable accommodation coordinators) to manage and track those requests.

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

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

f) 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.

g) *Any information sharing conducted by the system*

ETK EEO is accessible to authorized users within OCR and the bureau EEO Offices at National Institutes of Standards and Technology (NIST), National Oceanic Atmospheric Administration (NOAA) and Census Bureau on a role and official need-to-know basis only.

ETK RA is accessible to authorized users within OCR and the bureau HR Offices at National Institutes of Standards and Technology (NIST), National Oceanic Atmospheric Administration (NOAA), and Census Bureau on a role-specific and official need-to-know basis only.

Both ETK EEO and ETK RA data that is uploaded can only be changed in accordance with the privileges provided by OCR. Access is limited to Reasonable Accommodation Coordinators, assigned to perform request processing and reporting tasks; the Department's Disability Program Manager and OCR Deputy Director, assigned to perform reporting and administrator tasks. The system provides a range of privileges established by the Program Administrators and include the visibility of data, read/write access, business rules, and administrator functions. Information within the system may also be shared with the Employment and Labor Law Division, OGC, and other federal agencies (EEOC and the Merit Systems Protection Board) as required for EEO case processing, but these entities do not have access to the system.

h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*

The authority for processing discrimination complaints within the Department of Commerce is delegated to the Director, Office of Civil Rights, by Department Organization Order (DOO) 20-10. The Department's internal discrimination complaint program is described by Department Administrative Order (DAO) 215-9. The authority for the Department's EEO complaint processing program is contained in the regulations of the EEOC at 29 CFR § 1614, and policy guidance provided by EEOC Management Directive 110.

Related laws and regulations governing the Department's authority to process complaints of discrimination include 42 U.S.C. 2000e-l 6; 29 U.S.C. 633a; 29 U.S.C. 791 and 794a; 29 U.S.C. 206(d); E.O. 10577, 3 CFR 218 (1954-1958 Comp.); E.O. 11222, 3CFR 306 (1964-1965 Comp.); E.O. 11478, 3 CFR 133 (1969 Comp.); E.O. 12106, 44 FR 1053 (1978); and Reorganization Plan No. 1 of 1978, 43 FR 19807 (1978).

The authority for processing request for Reasonable Accommodations within the Department of Commerce is delegated to Reasonable Accommodation Coordinators in the Bureau's

Human Resources and OCR, by Department Administrative Order (DAO) 215-10. The Department's procedures for providing reasonable accommodations is also described in Department Administrative Order (DAO) 215-10. The authority for the Department's Reasonable Accommodation program is contained in the Rehabilitation Act of 1973, as amended; Executive Order (E.O.)13164, Establishing Procedures to Facilitate the Provision of Reasonable Accommodation (RA), dated July 26, 2000; 29 United States Code (U.S.C.) Section 791 et seq.; 29 Code Federal Regulations (CFR) Part 1614.203; Title I (Employment) of the Americans with Disabilities Act (ADA) of 1990, as amended, 42 U.S.C. §§ 12101 *et seq.*; 29 C.F.R. part 1630; and the Americans with Disabilities Act Amendments Act (ADAAA) of 2008, PL 110-325 (S. 3406); EEOC Revised Enforcement Guidance: Reasonable Accommodation and Undue Hardship Under the ADA, dated October 2002; EEOC Policy Guidance on E.O. 13164, dated October 2000.

i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system: Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
__X_ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	X
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	X
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.

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015).
____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	X
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID	X				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	X	h. Date of Birth	X	o. Financial Information	
b. Maiden Name		i. Place of Birth	X	p. Medical Information	X
c. Alias		j. Home Address	X	q. Military Service	
d. Gender	X	k. Telephone Number	X	r. Criminal Record	
e. Age	X	l. Email Address	X	s. Physical Characteristics	
f. Race/Ethnicity	X	m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion	X		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History			
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information	X		
k. Other work-related data (specify): Personnel actions and employment information as they relate to the matters underlying the complaint.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs		g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	

b. IP Address		d. Queries Run	X	f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)
Narrative information regarding claims of discrimination and request for reasonable accommodation.
Costs associated with investigations and reasonable accommodations.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	X	Hard Copy: Mail/Fax	X	Online	X
Telephone	X	Email	X		
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): DOC unions, if the union is representing an employee.					

2.3 Describe how the accuracy of the information in the system is ensured.

ETK EEO master administrators will audit the data that is entered into the system on a quarterly basis to ensure accuracy. These systems must retain accurate data in order to ensure that EEO complaint data and reasonable accommodation data is accurate when reporting internally to agency leadership, when posting on DOC's public website as required under the No FEAR Act (EEO data), as well as in regulatorily required reports to external agencies, including to the EEOC (the Annual 462 Report, the Annual MD 715 Report, which contains EEO and RA data) and to Congress (Annual No FEAR Report, which includes formal complaint data).

ETK RA data will also be audited quarterly for accuracy and completeness by the respective bureaus that use ETK.

In addition, in ETK EEO data cannot entered into required fields until all the preceding field has been fully entered. This new feature will help minimize manual errors and will prevent a user from entering incomplete data.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. The following form is contained in ETK EEO records: OMB CONTROL NO. 0690-0015, DOC CD 545 Formal Complaint of Discrimination Form. However, the forms in ETK RA are not covered by the Paperwork Reduction Act.
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

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

X	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	X
For administrative matters	X	To promote information sharing initiatives	

For litigation	X	For criminal law enforcement activities	
For civil enforcement activities	X	For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Regulatory reporting requirements – EEOC, Annual Report of Complaint Activity (462), No FEAR Act Reporting (annual and quarterly), MD 715 Part J Reporting purposes.			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

EEO complaints are filed by employees of the Department and applicants seeking employment contact information for the complainant (attorney/representative/union representative) and representatives (OGC's attorney assigned to the case) for either the complainant or the Department. This provides both parties (individuals working with the complainant and the Department representatives with the notices, reports, decisions, and supporting documents related to the complaint. A complainant is required to provide the demographic and employment information relevant to his or her claim of discrimination. This enables OCR to determine if the complaint meets procedural and/or jurisdictional requirements necessary to direct the scope of the investigation and adjudication of the complaint, which is directly related to OCR's core mission of enforcing nondiscrimination laws.

The BII maintained in ETK EEO contains contact information about law firms, unions and other agencies that represent each individual complainant. Other BII identifies the following: name of the firm contracted to investigate the case, name and contact information of the assigned subcontractor, and the costs associated with the investigation. This category of BII allows OCR to manage its investigative contracts to ensure costs allocated are controlled appropriately. Investigations contractors and subcontractors do not have access to ETK EEO.

PII and BII in ETK EEO are disseminated only within the framework of administrative complaint processes, and/or related litigation in federal court. Information is provided to the OGC's Employment and Labor Law Division, EEOC, Merit Systems Protection Board and/or Assistant U.S. Attorneys on a case-by-case basis. PII may also be shared with the servicing Human Resources Office (SHRO) to the extent required to carry out personnel actions ordered as corrective action, or the agreed terms for settlement.

Statistical data from the system is annually provided to the EEOC, the Office of Personnel Management, the Department of Justice, and selected members of Congress in compliance with the No FEAR Act and the EEOC Form 462 report.

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 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.

ETK RA users are RACs who can also run reports that identify the costs of all reasonable accommodations for the Department, for the bureau, the types of accommodations, the number of accommodations that are approved, denied or where an alternative accommodation is offered/provided. However, this information is generally provided in the aggregate, without names of requestors. General statistical data about reasonable accommodations may also be submitted by the Department to the EEOC as part of the annual Management Directive 715 Report (Part J) or to respond to questions posed to the Department by the EEOC regarding the agency's Disability Employment/Reasonable Accommodation Programs. One of the most important data points tracked through ETK RA by OCR will be the timeframes associated with processing all requests. All requests must be processed within the timeframes established under the Departments DAO 215-10, Processing Requests for Reasonable Accommodation.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Insider threat is possible. User access in ETK EEO is monitored and controlled by two master administrators within the Office of Civil Rights. ETK EEO User access is also controlled by the Master Administrators. They approve/deny requests for new users; purge users who separate from the agency or no longer need access. The controls are documented in the ETK EEO/RA Systems Account Management Policy. In addition, in ETK EEO most of the ETK EEO users have access only to their bureau's data. Similar to ETK EEO, ETK RA also has two master administrators who control access to ETK RA.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	X		X
DOC bureaus	X		X

Federal agencies	X		
State, local, tribal gov't agencies			
Public			
Private sector	X		
Foreign governments			
Foreign entities			
Other (specify): DOC Unions if union is representing Complainant.	X		

	The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
X	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	X*	Government Employees	X
Contractors	X**		
Other (specify): Other (specify): General Public for ETK RA means non-Federal applicants for DOC and Bureau jobs. "Contractors" refers to Tyler Technologies (formerly MicroPact Engineering), the vendor that hosts and maintains the system.			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: .	
X	Yes, notice is provided by other means.	Specify how: Notice is provided on form Complaint of Employment Discrimination Form (CD-498), which contains a Privacy Act notice. The information in ETK EEO is directly provided from the claimant, on the above noted form, who files a complaint against the Department. This also applies to request for reasonable

		accommodation when using the Request for Reasonable Accommodation Form (CD-575).
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: For ETK EEO, the complainant can decline to provide PII/BII when he or she completes the CD-498, but if they decline certain data points, the complaint may not be fully processed. For ETK RA, users have the option to decline use of the system to submit their requests and may still submit an RA request via an alternative method.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: When Complainants file their complaints using CD 498, they are informed that the PII/BII collected during the EEO complaints process to be used only for processing their complaint and for no other purpose. Similarly, with respect to ETK RA, if an employee or applicant uses the system to submit a request for RA, they are informed that that the PII/BII that is collected is only used in the processing of their RA request.
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: For ETK EEO, individuals may contact their servicing EEO Office or OCR for review and/or updates. For ETK RA, requestors may contact their servicing reasonable accommodation coordinator for review and/or updates.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: The system may only be accessed by authorized users entering a username issued by a program administrator and an encrypted password that must be changed every 90 days. Case visibility and read-write privileges are tailored to each user's bureau or office location and level of responsibility. The system also includes an "audit" capability that tracks change entries and edits by user, date, and time. Sessions terminate and users are automatically logged off if no activity occurs within 30 minutes.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): __07/25/2019_____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Entellitrak is available to federal agencies under FedRAMP via Platform as a Service (PaaS) and Software as a Service (SaaS) models. With FedRAMP certification, customers leverage MicroPact's secure cloud environment to store, process and protect sensitive data, using entellitrak. FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services and products. Entellitrak is also Accredited and Secure with C&A's based on NIST 800-53, DIACAP and DCID 6/3. MicroPact uses encryption for data at rest to our dedicated hosted customers. Our solution 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.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

__X_ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: EEOC GOV-1 https://www.gpo.gov/fdsys/pkg/FR-2002-07-30/pdf/02-18895.pdf and Commerce/Department 18 http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: NARA General Record Schedule 1
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
X	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	X	Overwriting	X
Degaussing		Deleting	X
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
X	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: Individual complainant information is identifiable and poses risks to integrity and confidentiality, leading to legal/financial exposure and risk to the Department's reputation.
X	Quantity of PII	Provide explanation: The volume of sensitive complaint information poses a substantial risk to the Department and individual complainants with respect to confidentiality and integrity, leading to legal/financial exposure and risk to the Department's reputation
X	Data Field Sensitivity	Provide explanation: ETK EEO is an EEO Complaint tracking system. EEO Complaint related EEO documents are collected and retained in the system, including Reports of Investigations (ROIs). If an EEO complaint is based on disability and has claims of failure to accommodate, then the case might have medical documentation to support the claim. This documentation is required in order to adjudicate the case.
X	Context of Use	Provide explanation: PII is used in the context of highly sensitive personal and workplace interactions, requiring preservation of confidentiality and integrity of the EEO and RA process.
X	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act and EEOC regulations require OCR to preserve the confidentiality of EEO complaint and RA requests information.
X	Access to and Location of PII	Provide explanation: EEO complaint and RA request information is only available on a strictly need-to-know basis.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data,

include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

As the number of users (35) who can access ETK is very limited and closely monitored by the master administrators in the Office of Civil Rights, potential threats to privacy are minimal. The data in ETK EEO/RA is secured and is FEDRAMPed. Users who forget their passwords and who are locked out have to contact the master administrators for assistance. Users who separate from the agency will no longer have access the system. The ETK EEO/RA Systems Account Management Policy outlines how the master administrators will manage User Access. The number of users will drop from 35 to 25 in 2022 when the Decennial Census winds down and is complete. ETK RA is very similar to ETK EEO as ultimately, both applications are built on FedRAMP certified Entelitrak platform. ETK RA eFile portal is a public portal where public users can self- register and submit requests for accommodations. The eFile role has very limited permissions in the eFIle system. eFilers can attach documents and notes and submit the requests for accommodations. They can only view the request they created. They cannot view RA requests submitted by other eFilers. All submitted requests are received and processed in the RA Tracker. eFilers do not have access to the RA Tracker system. The security in eFile and RA Tracker are enforced by role-based access control and hierarchy based permissions. ETK EEO will collect PII relating to medical documents that are part of an EEO complaint based on disability and failure to accommodate. The protections for this PII/medical documentation in ETK EEO are described in the first paragraph above.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

X	Yes, the conduct of this PIA results in required business process changes. Explanation: Users will be required to sign a confidentiality agreement.
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
X	No, the conduct of this PIA does not result in any required technology changes.