Template Version Number: 01-2022

U.S. Department of Commerce
Office of The Secretary

Privacy Impact Assessment
for the
Office of Workforce Relations
Entellitrak Employee Relations/ Labor Relations (ETK ER/LR)

Reviewed by: Tiffany Daniel, Bureau Chief Privacy Officer (BCPO)

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Concurrence of the BCPO (This is an existing information system that is eligible for an annual certification)

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.07.18 10:26:50 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date
(Or the BCPO if this is an existing system that is eligible for an annual certification)

U.S. Department of Commerce Privacy Impact Assessment
Office of Workforce Relations/Entellitrak Employee Relations/ Labor Relations (ETK ER/LR)

Unique Project Identifier: CSAM ID 3161

Introduction: System Description

The Entellitrak Employee Relations/Labor Relations (ETK ER/LR) Tracker is an automated, enterprise, web-based solution designed to track, manage, and report on Labor and Employee Relations case management for the Office of Human Resources. This system collects and maintains information for the Family Medical Leave Act (FMLA), Conduct and Performance-Based, Administrative and Negotiated Grievances, Collective Bargaining Agreements, Administrative Investigations, and Disciplinary actions.

The system includes hosting, maintenance, and support services from Tyler Technologies (The Cloud Service Provider). The ER/LR is an application information system providing a business need to have one case management system with business process flows built into it for both Employee Relations (ER) and Labor Relations (LR) organizations.

Provide a brief description of the information system.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
Major Application - Software as a Service (SaaS)

(b) System location
ETK ER/LR is included in the Tyler Federal Product Suite of Web-based applications which is currently hosted under a contract within an Equinix facility located at 44470 Chilum Place, DC3, building one (1), Ashburn, VA 20147. The system is used by the Department of Commerce, Office of Human Resources Management (OHRM), Office of Workforce Relations (OWR) in the Herbert C. Hoover Building, 1401 Constitution Avenue NW,

Washington DC 20230.

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

ETK ER/LR does not interconnect or exchange information with any other systems.

(d) The way the system operates to achieve the purpose(s) identified in Section 4

Employees contact employee relations specialists through various channels such as email, mail, phone, or in-person interactions. They contact these specialists when they need to file FMLA cases or a complaint against another employee or management official. Employees may contact these specialists if they have concerns about activities within an office that they believe might violate departmental regulations. In addition, Supervisors provide information and evidence that would necessitate opening a new case to be tracked. Case information is inputted into the system and case numbers are assigned. The system permits data to be reviewed and analyzed and options to run reports.

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

Information or cases can be retrieved by case number, individual's name, the name of the specialist who worked/ is working on that case, and by case type.

(f) How information is transmitted to and from the system

Case information is input into the system manually and are assigned case numbers. Information is not transmitted from the system.

(g) Any information sharing

SF50 information pertaining to the employee and the related case is disseminated only within the framework of the administrative complaint processes, and/or related administrative or litigation in federal court if requested. Information is provided to the Office of the General Counsel's (OGC) Employment and Labor Law Division on a case-by-case basis.

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

- The authority for processing allegations of harassment prohibited by Federal Law is described by Department Administrative Order (DAO) 202-955
- Probationary and trial Periods are described by DAO 202-315
- Performance Management System is described by DAO 202-430
- Administrative Grievance Procedure is described by DAO 202-771
- Discipline is described by DAO 202-751
- The Department of Organization Orders (DOO) 20-8 is for Director for Human Resources Management.
- 44 U.S.C. 3101 describes Records Management by Federal Agencies
- Executive Order (E.O.) 12107- Relating to the Civil Service Commission and labor- management in the Federal Service.

- Title 3U.S.C. 9 - Agency Chief Financial Officers.
- Title 44 U.S.D. 3101- Records Management by Agency Heads; general duties.

(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.
_____ 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	
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):					

_X_ 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.

____ This is an existing information system that is eligible for an annual certification, in which security and privacy controls are properly implemented, changes do not create new privacy risks and there is a SAOP approved Privacy Impact Assessment.

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*	X	f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
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: The employee relations specialists retrieve the complainant's SF-50 to follow actions that would be taken, and in certain actions. The SF-50 finalizes the action when warranted. The SF-50 finalizes the case that the ER Specialist was working on. It documents that whatever adverse action taken was completed and should be documented with the employees eOPF. The SF-50 contains the Social Security number of that employee.

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

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	X
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	
c. Work Address	X	g. Work History	X	k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information	X		
l. Other work-related data (specify): Retirement Plan Information					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	X
g. Other system administration/audit data (specify):					

Other Information (specify)

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	
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): National Finance Center (NFC) - United States Department of Agriculture (USDA)					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

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

To maintain the accuracy and integrity of the information stored in the ER/LR tracker, access is restricted to OWR HR Specialists only. Assigned in this branch are three (3) OWR HR Specialists with Administrative rights to include the OWR Director. This helps prevent modifications, or case deletions, within the ER/LR tracker and its data. Additionally, the OWR Director and Administrators perform audits and check of the ER/LR tracker to validate the accuracy of the information and address any discrepancies identified. This opportunity is also used to provide feedback regarding any inaccuracies or discrepancies the HR Specialists encounter while using the ER/LR tracker. Moreover, all OWR staff receive comprehensive training and resources on data entry best practices and guidelines provided by Tyler Technologies. Collectively these measures ensure consistent safeguarding and accurate data input.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
X	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	X
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):			

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).

PII could be provided by the employee, or it can be retrieved by the HR specialist within the OWR. PII is uploaded and maintained in the system.

The SF-50 information pertaining to the employee and the related case is disseminated only within the framework of the administrative complaint processes, and/or related litigation in federal court if requested. Information is provided to the OGC's Employment and Labor Law Division on a case-by-case basis.

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 ER/LR is monitored and controlled by three master administrators within the OWR. ER/LR User access is also controlled by the master administrators. They reach out to the service providers to create new user accounts, approve system user accesses, and purge users who separate from the agency or no longer need access. The OWR utilizes the PII information collected solely for cases as it pertains to the cases in support of the action that is being taken.

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		
DOC bureaus	X		
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Other (specify):			

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

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
X	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 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.

6.4 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		Government Employees	X
Contractors			
Other (specify): Only the Government employees within the OWR will have access to the IT system and the PII/BII.			

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: There is a warning banner displayed on the login page each time specialists access the system.
X	No, notice is not provided.	Specify why not: During case processing, specialists do not notify employees of their PII being collected. If the case is FMLA related, the employee provides their medical information in support of their FMLA case file. In such cases employees are aware they have provided their PII information. In cases where an employee files a complaint against another employee or management official, the OWR retrieves the SF-50 information to verify employee's employment information. All ETK ER/LR specialists are Human Resources (HR) specialists with authorized access to HR systems and a part of their regular duties is to access systems that contain PII and data specific to employees, their tenure, their salary, etc. There is no requirement that specialists should provide notice to employees when accessing an employee's PII.

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 cases pertaining to FMLA requests, Employees provide their own PII to the HR specialists. The employee could decline to provide their PII.
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: For cases where a complaint is filed against an employee or management official, an employee's employment information is collected when their SF-50 is retrieved by the HR specialists. Employees are not made aware that their PII has been retrieved and hence they do not have the opportunity to decline to provide their PII.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: For cases pertaining to FMLA requests, notice is provided on forms WH-380E and WH-380F that the employees' information will be used to determine their FMLA eligibility. Employees requesting FMLA provide their PII to the HR specialists to create the FMLA certification. Individuals do not have an opportunity to consent to uses of their PII, once they provide their PII information to an HR specialist, they are consenting to all uses of their PII pertaining to their FMLA request. For cases where a complaint is filed against an employee, that employee's employment information is collected when their SF-50 is retrieved. The SF-50 is also retrieved to determine years of service and federal employment status. employees are not made aware that their PII has been retrieved and hence they do not have the opportunity to consent to the particular uses of their PII.

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: With regards to FMLA instance, when the Office of Workforce Relations handles PII, the employee has the discretion to provide their medical documentation to OWR for review to determine FMLA eligibility. They also have the opportunity to update PII regarding FMLA at any time.
X	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: For cases where a complaint is filed against an employee, that employee's employment information is collected when their SF-50 is retrieved. The employee is not made aware that their PII has been retrieved and hence they do not have the opportunity to review or update PII pertaining to them.

Section 8: Administrative and Technological Controls

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

	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 a password that must be changed every 90 days. Case visibility and read-write privileges are tailored to each user's level of responsibility. The system also includes an "audit" capability that tracks changes of 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): ___May 27, 2024_____ ☐ 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 or higher.
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.
X	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 Software as a Service (SaaS) with FedRAMP certification, customers leverage Tyler Federal'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&As based on NIST 800-53, DIACAP and DCID 6/3. Tyler Federal 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)*: DEPT-1 System of Records Notices - COMMERCE-DEPT-1 | U.S. Department of Commerce DEPT-14 System of Records Notices - COMMERCE-DEPT-14 | U.S. Department of Commerce DEPT-18 System of Records Notices - COMMERCE-DEPT-18 | U.S. Department of Commerce OPM-3 OPM GOVT-3
	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: Yes. ER/LR files that relate to employee relation and labor relations are covered by the NARA GRS Schedule 2.3: Harassment complaint case files., Item 050 (DAA-GRS-2018-0002-0005) Employee Relations Records, Item 060 (DAA-GRS-2018-0002-0006) Administrative Grievances, Disciplinary, and Adverse Action Files; Item 130, Labor Management Relations Agreement Negotiations Records (DAA-GRS-2018-0002-0015)
	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		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 level. *(Check all that apply.)*

X	Identifiability	Provide explanation: Details information of employee work related data and system administration and audit data. 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: The ER/LR Tracker is an automated, enterprise, web-based solution designed to track, manage, and reports on Labor and Employee Relations case management for the Office of Human Resources. ER/LR collects sensitive data, such as medical information and social security numbers of employees. The loss of confidentiality or integrity could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
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 ER/LR process.
X	Obligation to Protect Confidentiality	Provide explanation: The Privacy Act and the U.S. Office of Personnel Management (OPM) guidance and regulations require the Office of Workforce Relations to preserve the confidentiality of ER/LR complaints and requests information.
X	Access to and Location of PII	Provide explanation: ER/LR complaints and FMLA 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.)

Individuals who have access to the information in the system are a limited number and are all employees in the Office of Workforce Relations, Office of Human Resources Management. Users are granted access to the information in the system based on their need-to-know. Users who forget their passwords and who are locked out must contact the master administrators for assistance. Users who separate from the agency will no longer have access the system. The ER/LR Systems Account Management Policy outlines how the master administrators will manage User Access.

For cases pertaining to FMLA requests, notice is provided on forms WH-380E and WH-380F that the employee's information will be used to determine their FMLA eligibility. Employees requesting FMLA provide their own PII to the HR specialists to create the FMLA certification. Also, the FMLA filer's SF-50 is retrieved by the HR specialists to determine years of Government service and federal employee entitlement. Only authorized users with the need to know have access to the PII information on the SF-50 forms.

For cases where a complaint is filed against an employee, The employee's employment information is collected when their SF-50 is retrieved. The SF-50 contains information about an employee's past and current government employment. Only authorized users with the need to know have access to the PII information on the SF-50 forms.

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

	Yes, the conduct of this PIA results in required business process changes. Explanation:
X	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.