

**U.S. Department of Commerce
U.S. Patent and Trademark Office**



**Privacy Impact Assessment
for the
General Counsel Case Tracking System Cloud (GCCTS-C)**

Reviewed by: Deborah Stephens, 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

NICHOLAS CORMIER Digitally signed by NICHOLAS CORMIER 9/19/2025
Date: 2025.09.19 13:55:38 -04'00'

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO General Counsel Case Tracking System Cloud (GCCTS-C)

Unique Project Identifier: EBPL-LT-06-00

Introduction: System Description

Provide a brief description of the information system.

General Counsel Case Tracking System - Cloud (GCCTS-C) is a legal practice management system used by the Solicitor's Office within the Office of the General Counsel (OGC). It is used for managing Intellectual Property litigation and prosecutions of practitioners who practice before the agency for ethics violations. These litigation cases include documents, activity dates, and contacts. The system allows the legal staff in the Solicitor's Office to store the case information and documents and track due dates for the attorneys and paralegals involved in each matter.

Address the following elements:

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

GCCTS-C is a major application.

(b) System location

Amazon Web Services (AWS East), Alexandria, VA.

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

GCCTS-C interconnects with the following systems:

Identity, Credential, and Access Management - Identity as a Service (ICAM-IDaaS) – mission is to provide an enterprise authentication and authorization service to all applications/AIS's.

PTO-EIPL-IHSC-UACS-USPTO AWS Cloud Services (UACS) –is an infrastructure platform used to support USPTO systems hosted in the AWS East/West environment. The UACS provides administrative efficiency, improves security, and provides better oversight across all applications which reside on the UACS platform.

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

GCCTS-C is a Commercial Off-The-Shelf (COTS) web application that allows authorized users to login using Single Sign-On from the web browser. After logging in, users can search and view existing legal cases or create a new case. Paralegals will typically create new cases when required and will add the assigned Attorneys to the case. All users can add or view metadata and documents for a case and can view a calendar of due dates and activity dates for a case and create new calendar entries. The case matter in the application provides a centralized location for the legal users to track and view the case from inception to completion. Closed cases are kept in the system until they are transferred to archives and/or disposed of, per records management policy.

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

GCCTS-C is a web-based application that allows authorized internal users to access and view information in the system using a web browser. After logging in, users have role-based access permissions that allow them to search and view existing legal cases and documents that they have permissions for.

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

Information is transmitted to the system via upload from the users desktop. Users can transmit data from the system by downloading it to the desktop.

(g) Any information sharing

The GCCTS-C system is largely a repository of Intellectual Property legal case information and documents which may also be shared with other USPTO employees, Department of Commerce attorneys, Department of Justice attorneys, opposing counsel, public individuals directly involved with a legal matter, and the U.S. Federal District and Appellate Courts.

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

35 USC § 2(b)(2)(D) [Patent Practitioners],
 35 USC § 6 [PTAB proceedings],
 37 CFR § 11 Subpart C– [Investigations and Disciplinary Proceedings; Jurisdiction, Sanctions, Investigations, and Proceedings]

(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):					

☐ 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.

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	☒
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☐	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☒				
n. Other identifying numbers (specify): USPTO Customer Number, Patent application number, Trademark serial number					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☐	o. Financial Information	☒
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☒
c. Alias	☐	j. Home Address	☒	q. Military Service	☐
d. Sex	☐	k. Telephone Number	☒	r. Criminal Record	☒
e. Age	☐	l. Email Address	☒	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	☒	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	☐	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	☒	k. Procurement/contracting records	☐
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
l. Other work-related data (specify):					

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	☐
g. Other system administration/audit data (specify):					

Other Information (specify)					
The cases in the GCCTS-C system include documents involving grievances that are being investigated. We do not have control of what information might be included in associated documents that are stored as part of the legal case.					

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	☒	Hard Copy: Mail/Fax	☒	Online	☒
Telephone	☒	Email	☒		
Other (specify):					

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

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.

The accuracy of the information is ensured by receiving it directly from the individuals or some USPTO systems that received the information directly from the individuals with whom the information pertains. The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

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.
☒	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):			

☒	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): Click or tap here to enter text.			

☒	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	☐
For administrative matters	☒	To promote information sharing initiatives	☒
For litigation	☒	For criminal law enforcement activities	☐
For civil enforcement activities	☐	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).

The stored PII may include portions or all references in Section 2.1 for Identifying Numbers, General Personal Data, and Work-Related Data. The data is for internal Solicitors Office staff use only that supports legal case and document management and may contain confidential patent application information, court documents under seal, and sensitive prosecution information that is not releasable to the public. The information may reference federal employees, members of the public, discipline of practitioners, and foreign nationals.

USPTO employees and contractors with access to system – User Id, name, email for their user accounts and to keep track of individuals handling the case.

Practitioners – Name, Taxpayer Id, Financial Account, Financial Transaction, File/Case Id, USPTO Customer Number, Patent application number, Trademark serial number, Financial Information, Home Address, Telephone Number, Email Address, Education, Medical Information, Criminal Record, Occupation, Job Title, Work Address, Work Telephone Number, Work Email Address, Work History, Business Associates, Proprietary or Business Information is for identification of practitioner that would be involved in a disciplinary proceeding.

Other members of the public - Name, File/Case Id, Patent application number, Trademark serial number, Home Address, Telephone Number, Email Address, Occupation, Job Title, Work Address, Work Telephone Number, Work Email Address, Business Associates, Proprietary or Business Information is for the identification of parties involved in IP litigation defending agency decisions and representing the agency Director in district court actions.

- 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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

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

☐ 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.
☐	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: ICAM-IDaaS NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
☐	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	☒
Contractors	☒		
Other (specify):			

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.)*

☒	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:	
☒	Yes, notice is provided by other means.	Specify how: This PIA serves as notice.
☐	No, notice is not provided.	Specify why not:

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

☐	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: USPTO employees and contractors do not have the opportunity to decline to provide PII/BII into this system as it is needed for them to perform their duties. For members of the public, including patent/trademark practitioners do not have an opportunity to decline to provide PII/BII as it is needed to process any litigation.

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:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The GCCTS application requires the login ID and name to authenticate and identify the individuals in the application.

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

☐	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: USPTO employees and contractors do not have the opportunity to review or update the PII/BII pertaining to them within this system but they have the opportunity to review and update their personal information online through NFC's Employee Personal Page application or the Department of Treasury's HR Connect system. Employees may also visit the USPTO's Office of Human Resources (OHR) department

		for additional assistance. These updates will change the information within Active Directory to update the users' access privileges. The individuals involved in litigation do not have the opportunity to update their PII within the system. They do not have access to the system and do not have an opportunity to see their information in the system. If a document contains incorrect information, they can request that their information be updated via email or mail.
--	--	---

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.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit Logs
☒	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): ☒ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 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).
☐	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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

Section 9: Privacy Act

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

☒ 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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i> PAT-TM-1, Attorneys and Agents Recognized to Practice Before the Office PAT-TM-2, Complaints, Investigations and Disciplinary Proceedings Relating to Attorneys and Agents Registered or Recognized to Practice Before the Office DEPT-14, Litigation, Claims, and Administrative Proceeding Records
☐	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
☐	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.)*

[General Records Schedules \(GRS\)](#) | [National Archives](#)

☒	There is an approved record control schedule. Provide the name of the record control schedule: Agency Precedential Court Cases: N1-241-09-1:b1.1 Solicitor's Office Records Related to Non-Precedential Court Cases: N1-241-09-1:b1.2 Non-Administrative IP Law Internal Management, Program, and Subject Files: N1-241-09-1:b1.4 Administrative Law Files, Office of Enrollment and Discipline Appeal Case Files: N1-241-09-1:b4.5 General Technology Management Records - Information technology operations and maintenance records – GRS 3.1:020 - Including System logs – Temporary: Destroy 3 years after (See GRS for cutoff instructions). Information Systems Security Records - GRS 3.2
☐	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:
☒	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	☐
Degaussing	☐	Deleting	☒
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.
☒	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.)*

☒	Identifiability	Provide explanation: GCCTS collects, maintains, or disseminates PII about DOC employees and contractors. The
-------------------------------------	-----------------	--

		types of information collected, maintained, used or disseminated by the system include name, address, email, and phone. When combined, this data set can be used to identify a particular individual.
☒	Quantity of PII	Provide explanation: The quantity is limited to the amount and type of requests received by the business unit and is moderate. A serious or substantial number of individuals would be affected by loss, theft, or compromise.
☒	Data Field Sensitivity	Provide explanation: The combination of name, home address, telephone number, and email address do not make the data fields any more sensitive because they are publicly available information.
☒	Context of Use	Provide explanation: Data includes name and personal and work name, telephone number and email address as well as user ID and date/time access for purposes of case management.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: GCCTS is a web application that allows authorized users to access and view information in the system using a web browser. Access is limited to authorized personnel only, government personnel, and contractors.
☐	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.)

In addition to insider threats, activity which may raise privacy concerns include the collection, maintenance, and dissemination of PII in the form of personal and work-related data such as name, telephone number and email address as well as user ID and date/time access. USPTO mitigates such threats through mandatory training for system users regarding appropriate handling of information and automatic purging of information in accordance with the retention schedule.

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:
☒	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:
☒	No, the conduct of this PIA does not result in any required technology changes.