

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



**Privacy Impact Assessment
for the
Enrollment and Discipline Information Technology System (EDITS)**

Reviewed by: Henry J. Holcombe, 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

CHARLES CUTSHALL

Digitally signed by CHARLES CUTSHALL
Date: 2024.01.02 13:03:31 -05'00'

4/13/2023

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Enrollment and Discipline Information Technology System (EDITS)

Unique Project Identifier: EBPL-LT-05-00

Introduction: System Description

Provide a brief description of the information system.

Enrollment and Discipline Information Technology System (EDITS) is a major application which will be the cloud replacement of the existing on-premise Corporate Imaging Document (CIDM) subsystem of the PTO-AASS-Agency Administrative Support System. EDITS is a repository of imaging documents serving the USPTO Office of Enrollment and Discipline (OED) where documents are stored, made searchable, and retrievable via USPTO Office of Enrollment and Discipline Information System (OEDIS). The documents stored are related to individuals applying for registration to practice in patent matters before the USPTO and registered patent practitioners.

Address the following elements:

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

(b) *System location*
Alexandria, Virginia

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

Intellectual Property Leadership Management System (IPLMSS) - is a Major Application information system, which provides the capabilities and functionality.

USPTO AWS Cloud Services (UACS) - is a standard infrastructure platform used to support PTO Application Information Systems (AIS) hosted in the AWS East/West environment.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*
EDITS is a document management system that meets user requirements and conforms to USPTO system infrastructure requirements specified by the Chief Information Officer (CIO).

EDITS provide similar document management requirements and functionalities to Office of Enrollment and Discipline (OED).

There are two ways of using EDITS: the first is through its connection with OEDIS where OEDIS serves as the user interface and secondly through a simplified UI that EDITS provides. The simplified UI has limited capabilities compared to the OEDIS connection. Authentication is implemented using OKTA, credentials are managed using Secrets Manager, Textract service is used to extract text from scanned documents/images, search functionality is implemented using Open Search. PostgreSQL is used to store metadata associated with documents/images. EDITS software changes follow the USPTO DevSecOps Change Management Policy and USPTO DevSecOps Change Management Procedures.

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

Information in EDITS is retrieved via USPTO intranet access via registered accounts. EDITS will offer a web browser application where files can be searched and retrieved by a small group of OED employees (Analytical Team). Additionally, documents stored in EDITS can be retrieved, searched, and uploaded through OEDIS-Core (internal) and uploaded through OEDIS-CI (external).

EDITS is made accessible as follows:

4. OEDIS-CI (Customer Interface) used by external customers (public facing) for uploading and downloading documents uploaded by the external interface;
5. Through OEDIS-Core (internal) application for internal usage;
6. Through EDITS own web interface.

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

Information is encrypted and transmitted to EDITS via Hyper Text Transfer Protocol Secure (HTTPS) and Secure Shell (SSH).

(g) Any information sharing

EDITS shares PII within the agency and DOC bureaus on a case by case basis.

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

37 CFR §§ 11.5 through 11.11 and America Invents Act

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

EDITS is a Moderate system.

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	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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*	<input checked="" type="checkbox"/>	f. Driver's License	<input checked="" type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
b. Taxpayer ID	<input checked="" type="checkbox"/>	g. Passport	<input checked="" type="checkbox"/>	k. Financial Transaction	<input checked="" type="checkbox"/>
c. Employer ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input checked="" type="checkbox"/>	l. Vehicle Identifier	<input checked="" type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	i. Credit Card	<input checked="" type="checkbox"/>	m. Medical Record	<input checked="" type="checkbox"/>
e. File/Case ID	<input checked="" type="checkbox"/>				
n. Other identifying numbers (specify): Credit card includes just the last 4 digits of the credit card number. The system may include other PII that users have voluntarily submitted.					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: Social Security numbers are not actively collected by the system. Legacy documents may or may not have truncated social security numbers.					

General Personal Data (GPD)

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

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

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input checked="" type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input checked="" type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input checked="" type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input checked="" type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input checked="" type="checkbox"/>	j. Weight	<input checked="" type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. Other distinguishing features/biometrics (specify): Recordings from investigations can be transcribed to PDF.					

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input checked="" type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	f. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input checked="" type="checkbox"/>
g. Other system administration/audit data (specify): EDITS inherits most of the auditing from interfacing systems such as OEDIS and AD. There is also internal auditing done by AWS and the application.					

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	<input checked="" type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input checked="" type="checkbox"/>	Other Federal Agencies	<input checked="" type="checkbox"/>
State, Local, Tribal	<input checked="" type="checkbox"/>	Foreign	<input checked="" type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input checked="" type="checkbox"/>	Private Sector	<input checked="" type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input checked="" type="checkbox"/>		
Other (specify): College of Patent Agents and Trademark Agents (CPATA), a Canadian entity.					

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

The accuracy of the information in the system is ensured by obtaining most of the PII/BII directly from the individual before it is transferred to EDITS. The individual may request to review any PII/BII within the system that pertains to them and request an update if it is not accurate. When PII/BII within the source system is updated, the PII/BII within EDITS will be updated.

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?

<input checked="" type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. 0651-0012 Admission to Practice 0651-0017 Practitioner Conduct and Discipline 0651-0081 Law School Clinic
<input type="checkbox"/>	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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify): Click or tap here to enter text.			

There are not any IT systems 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	<input type="checkbox"/>	For administering human resources programs	<input type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input checked="" type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
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).

OEDIS and EDITS are systems supporting the efforts of The Office of Enrollment and Discipline (OED). OED administers the registration exam and maintains a roster of current patent practitioners. OED also investigates grievances submitted against practitioners, provides public information about disciplinary actions against practitioners, coordinates a nationwide Patent Pro Bono Program for under-resourced inventors seeking free legal help, and administers a Law School Clinic Certification Program where law students gain experience in intellectual property law. Reason: Certain types of PII/BII are collected in the application process for individuals applying for registration to practice in patent matters before the USPTO and roster maintenance of existing registered patent practitioners. Additionally, certain types of PII/BII can be requested and collected during the course of investigating grievances submitted against practitioners. Certain types of PII/BII can be requested in the event an individual is requesting reasonable accommodation. Other types of PII/BII may not be requested by OED but could be received and stored.

- 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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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?

<input type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input checked="" type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>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:</p> <p>IPLMSS</p> <p>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.</p>
<input type="checkbox"/>	<p>No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.</p>

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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.)*

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	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: https://www.uspto.gov/privacy-policy	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

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

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: The PII/BII within EDITS is obtained from OEDIS. Individuals do not have the opportunity to decline to provide their PII/BII. The PII/BII requested is the minimum amount necessary for the individuals to become registered to practice in patent matters before the USPTO and registered patent practitioners.

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

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals do not have an opportunity to consent to particular uses of their PII/BII. The PII/BII is necessary for the functionality of the system.

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

<input type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: Individuals do not have direct access to EDITS. Certain documents submitted through OEDIS – applicant portal, that are stored in EDITS, will be viewable only.

Section 8: Administrative and Technological Controls

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

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit logs
<input checked="" type="checkbox"/>	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): <input checked="" type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.

<input checked="" type="checkbox"/>	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).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish DOC ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	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).

All access has role-based restrictions and individuals with access privileges undergo vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access. The data is encrypted in transit and at rest. Additionally, EDITS is secured by various USPTO infrastructure components, including the NSI system and other OCIO established technical controls to include password authentication at the server and database levels.

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.”

<input checked="" type="checkbox"/>	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. (list all that apply):</p> <p>PAT/TM-1 Attorneys and Agents Registered or Recognized to Practice Before the Office</p> <p>PAT/TM-2 Complaints, Investigations and Disciplinary Proceedings Relating to Attorneys and Agents Registered or Recognized to Practice Before the Office</p> <p>PAT/TM-5 Non-Registered Persons Rendering Assistance to Patent Applicants</p> <p>COMMERCE/DEPT-25 Access Control & Identity Management Systems</p> <p>COMMERCE/DEPT-31 Public Health Emergency Records of Employees, Visitors, and Other Individual</p>
-------------------------------------	---

	Department Locations
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule: N1-241-09: 1:b4.2 Enrollment and Discipline Application and Roster Maintenance Files
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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	<input type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.)*

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

<input checked="" type="checkbox"/>	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.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: SSN, name, date of birth, email address, credit card and medical records can be used to identify an individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: Around 60,000 practitioners and a few thousand applicants. For each of those we have dozens of PII points that include sensitive PII.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: Disclosure or unauthorized access will have a major impact on the organization.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: EDITS is designed to serve as a consolidation of document imaging serving the USPTO Office of Enrollment and Discipline (OED).
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: S3, the AWS storage bucket (e.g. file storage system), will contain all the PII. Access will be determined by OKTA (authentication) and authorization by the metadata stored in RDS (the postgres SQL database).
<input type="checkbox"/>	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.)

USPTO has also identified and evaluated potential threats to PII such as insider threats and adversarial entities which may cause a loss of confidentiality, accessibility and integrity of information. Users are provided one-on-one, weekly, and monthly training. All users have access restriction or permissions based on the built-in security controls of the system. Furthermore, the system has the ability to password protect any sensitive data for added protection. Data retention is managed automatically using IQ Archivist in accordance with records management retention policy. System access to PII/BII data is limited to a restricted set of users.

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

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	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.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.

PRIVACY ACT STATEMENT

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.