Template Version Number: 01-2021

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: 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
Date: 2026.08.06 11:09:15 -04'00' 8/6/2026

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 serving the Office of Enrollment and Discipline (OED). It includes the components OEDIS (Office of Enrollment and Discipline Information System) and EDITS-DMS (Enrollment and Discipline Information Technology System - Document Management System).

The OEDIS component has an internal application that supports the United States Patent and Trademark Office (USPTO) in meeting statutory obligations related to the application, registration, maintenance, and discipline of patent practitioners. OEDIS also has a public facing application which allows members of the public to search for registered practitioners, enables applicants and patent practitioners to update their contact information, submit requests to the USPTO and pay fees online, and manage their applications and registrations.

The EDITS-DMS component provides a searchable repository of imaging documents for the OEDIS component. The documents are related to individuals applying to become patent practitioners and those who are registered patent practitioners.
Address the following elements:

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

Major Application

(b) System location

Amazon Web Services (AWS US East 1), Ashburn, VA.

(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:

Data Delivery System (DDS) - IDaaS provides unified acess management across applications and API based on single sign-on service. Identity and access management is provided by Okta's cloud-based solution which uses Universal Directory to create and manage users and groups.

Fee Processing Next Generation (FPNG) - This system provides USPTO customers services for the online payment of fees related to Patent and Trademark business.

MyUSPTO Cloud - The USPTO is transitioning users to a single secure uspto.gov account, managed through MyUSPTO, to simplify sign-in and personalize access for individual users, with future enhancements planned for organizational sharing.

Open Data/Big Data Master System (OD/BD MS) - The USPTO Developer Hub provides public access to USPTO data, APIs, analytics, visualizations, feeds, and adjudicatory documents by ingesting and publishing data from multiple sources, managing website content in Drupal, and linking to additional USPTO-hosted APIs.

Cloud System Performance Monitoring (CloudSPM) - Cloud System Performance Monitoring provides real-time observability and instrumentation across cloud and non-cloud environments to help USPTO optimize performance, utilization, availability, troubleshooting, and recovery for critical IT infrastructure and applications, including tools such as AECAS, SAAM, and Splunk Heavy Forwarders.

ICAM Identity as a Service (ICAM-IDaaS) - Enterprise authentication and authorization service to all applications/AIS's.

Enterprise Desktop Platform (EDP) - Standard enterprise-wide environment that manages desktops and laptops providing USPTO.

USPTO AWS Cloud Services (UACS) - Operational Guidelines and Policies for USPTO Components deployed to the USPTO UACS environment

Network and Security Infrastructure System (NSI) - Is an Infrastructure information system which provides an aggregate of subsystems that facilitate the communications, secure access, protective services, and network infrastructure support for all USPTO IT applications.

Unified Generative AI Platform UMACS (UGAP-UMACS) - UMACS IaaS initiative is part of the ongoing Enhanced Platform Automation (EPA).

Patent Capture and Application Processing System - Examination Support (PCAPS-ES) - OEDIS provides data to OPSG within PCAPS-ES.

Enterprise Software Services (ESS) - On AWS Adobe Experience Manager (AEM) is utilized to manage XFA and PDF form routing and signatures. Currently, TMNG-eFile and TMNG-eOG uses AEM On AWS. ISB team maintains the servers, software and ATO for AEM On AWS.

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

EDITS-DMS is a document management system that meets user requirements and conforms to USPTO system infrastructure requirements specified by the Chief Information Officer (OCIO). EDITS-DMS provides similar document management requirements and functionalities to OEDIS.

There are two ways of using EDITS-DMS: the first is through its connection with OEDIS where OEDIS serves as the user interface and secondly through a simplified UI that EDITS-DMS provides. The 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-DMS offers 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-DMS can be retrieved, searched, and uploaded through OEDIS-Core (internal) and uploaded through OEDIS- Customer Interface (CI) (external).

EDITS is made accessible as follows:
1. OEDIS-CI used by external customers (public facing) for uploading and downloading documents uploaded by the external interface;
2. Through OEDIS-Core (internal) application for internal usage;
3. Through EDITS-DMS 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 representational state transfer application programming interface (API) Transport Layer Security (TLS) 1.3.

(g) Any information sharing

The OED evaluates applicants for admission to the patent bar and investigates allegations of misconduct by practitioners who practice before the USPTO. It is primarily within these two contexts that OED gathers documentation. These documents contain, among other things, attorney work products, PII and BII. Upon request, OED may share this documentation internally and externally, typically on a case-by-cases basis, and subject to restrictions such as the Privacy Act and the USPTO System of Records Notices.

(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

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): 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	☒	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): Recordings from investigations can be transcribed to PDF.					

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): 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	☒	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): 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/Business Identifiable Information (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 Information Technology (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. 0651-0012 Admission to Practice 0651-0017 Practitioner Conduct and Discipline 0651-0081 Law School Clinic
☐	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).

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	☒	☐	☒
DOC bureaus	☒	☐	☐
Federal agencies	☒	☐	☐
State, local, tribal gov't agencies	☒	☐	☐
Public	☒	☒	☒
Private sector	☒	☐	☐
Foreign governments	☒	☐	☐
Foreign entities	☒	☐	☐
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.
☐	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: DDS FPNG MyUSPTO Cloud OD/BD MS CloudSPM ICAM IDaaS EDP UACS

	NSI UGAP UMACS PCAPS-ES ESS 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: https://www.uspto.gov/privacy-policy	
☒	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: 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.

☐	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: 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.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals have an opportunity to download their own submitted application packages through OEDIS-CI. Applicants and Practitioners may request a copy of their files. Applicants and Practitioners are able review and update their profile information using OEDIS-CI.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

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

☒	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): 5/29/2025

	☐ 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).*

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 Office of the Chief Information Officer (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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: PAT/TM-1 Attorneys and Agents Registered or 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 PAT/TM-5 Non-Registered Persons Rendering Assistance to Patent Applicants
☐	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.)*

General Records Schedules (GRS) | National Archives

☒	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** N1-241-09-1, b4.7 b-4-7 **Enrollment and Discipline Roster of Attorney's and Agents Registered to Practice Before the USPTO** Lists of practicing attorneys and agents registered for USPTO practice and in good standing. Also includes ledgers containing registration numbers of those attorneys and agents from 1897 to the present time, and records of complaints against those attorneys and agents. Temporary: Destroy when superseded. N1-241-09-1, b4.8 b-4-8 **Director's OED Decision Files** Reference copies of non-interlocutory decisions issued by the Commissioner for examination regrades, denials of entry, Office of Enrollment and Discipline (OED) disciplinary hearings or decisions, determinations of technical and scientific qualifications, and to practice before the USPTO. Used by OED staff for reference purposes. Temporary: Destroy when no longer needed for current USPTO business. **GRS 3.1**: **General Technology Management Records** Item - 020 Information technology operations and maintenance records. Which include access and audit logs. **GRS 3.2. Information Systems Security Records**, Item 010, 020, 040, 050 Which include system security logs.
☐	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: SSN, name, date of birth, email address, credit card and medical records can be used to identify an individual.
☒	Quantity of PII	Provide explanation: Over 60,000 practitioners and several thousand applicants. For each of those we have dozens of PII points that include sensitive PII.
☒	Data Field Sensitivity	Provide explanation: Disclosure or unauthorized access will have a major impact on the organization.
☒	Context of Use	Provide explanation: EDITS is designed as the main system for the USPTO Office of Enrollment and Discipline (OED).
☒	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.
☒	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 USPTO AWS Cloud Services (UACS) Relational Database Service (RDS PaaS) (Postgres Structured Query Language (SQL) database)
☐	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.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical and logical access to servers are restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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.