Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Enrollment and Discipline Information Technology System (EDITS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Enrollment and Discipline Information Technology System (EDITS)

Unique Project Identifier: EBPL-LT-05-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 purpose that the system is designed to serve

EDITS is designed to serve as a consolidation of document imagining serving the USPTO Office of Enrollment and Discipline (OED). OED imaging documents are made searchable and retrievable via the OEDIS. EDITS is an AWS cloud-based solution that supports the Office of Enrollment and Discipline Systems - OEDIS-Core (internal) and OEDIS-CI (external customer interface) of the USPTO by providing a repository for storing documents/images, web services to facilitate upload/download of documents/images with associated metadata, OCR capability to extract text from scanned documents/images, and User Interface (UI) to facilitate search functionality.

e) *The way the system operates to achieve the purpose*

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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

EDITS may include PII collected, stored, maintained, used, or disseminated about individuals applying for registration to practice in patent matters before the USPTO, registered patent practitioners, USPTO employees, and contractors. PII about USPTO employees and contractors

could include information such as name, employee ID and other work-related data. Information collected about registered patent practitioners and prospective patent practitioners include identifying numbers, work related data, general personal data, and distinguishing features. EDITS collect system administration and audit data such as user ID and date and time of access information.

g) Identify individuals who have access to information on the system

USPTO employees and contractors.

h) 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:

1. OEDIS-CI (Customer Interface) 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 own web interface.

i) 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).

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☒ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☐ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☒ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☐ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

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

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is]

privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☒ Yes, the IT system collects, maintains, or disseminates BII.

☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

- ☒ DOC employees
- ☒ Contractors working on behalf of DOC
- ☒ Other Federal Government personnel
- ☒ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☒ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form. The system will not collect nor ask for SSNs but there are legacy documents that could have SSNs or partial SSNs.
Provide the legal authority which permits the collection of SSNs, including truncated form. 0651-0012 – Admission to Practice 37 CFR 1.21, 10.14, and 11.5-11.11

☐ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☒ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☐ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the Enrollment and Discipline Information Technology System (EDITS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Enrollment and Discipline Information Technology System (EDITS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Kevin Donahoe Office: CFO/IDPD Phone: (571) 272-5123 Email: Kevin.Donahoe@uspto.gov Signature: Users, Donahoe, Kevin Digitally signed by Users, Donahoe, Kevin Date: 2023.02.17 17:26:40 -05'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2023.02.28 15:57:08 -05'00' Date signed: _____
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2023.02.24 11:09:14 -05'00' Date signed: _____	**Bureau Chief Privacy Officer and Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.03.01 09:47:36 -05'00' Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: _____ Date signed: _____	