Version Number: 01-2019

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

Privacy Threshold Analysis
for the
Information Delivery Product (IDP)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Information Delivery Product (IDP)

Unique Project Identifier: PTOC-003-00

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 and its purpose: *Provide a general description system (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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).

a) Whether it is a general support system, major application, or other type of system
Information Delivery Product (IDP) is a Major Application within USPTO.

b) System location
IDP resides at the USPTO facilities located in Alexandria, Virginia.

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

- Network and Security Infrastructure System (NSI)
- Corporate Administrative Office System (CAOS)
- Enterprise Software Services (ESS)
- Enterprise Unix Services (EUS)
- Enterprise Windows Services (EWS)
- Service Oriented Infrastructure System (SOI)
- Consolidated Financial System (CFS)
- Enterprise Desktop Platform (EDP)
- Patent Capture and Application Processing System –Examination Support (PCAPS-ES)
- Agency Administrative Support System (AASS)
- Fee Processing Next Generation (FPNG)

- Patent Trial and Appeal Board End to End (PTAB-E2E)
- Enterprise Records Management and Data Quality System (ERMDQS)
- Corporate Web Systems CWS)
- Database Services (DBS)

d) The purpose that the system is designed to serve

IDP is a Master System composed of the following three (3) subsystems: 1) Enterprise Data Warehouse (EDW), 2) Electronic Library for Financial Management System (EL4FMS), and 3) Financial Enterprise Data Management Tools (FEDMT).

EDW: is a United States Patent and Trademark Office (USPTO) system providing access to integrated USPTO data through various tools in support of not only reporting and visualizing but also analytics used in decision-making across USPTO.

EL4FMS: is an automated information system (AIS) that provides access to USPTO financial-related documents to support the decision-making activities of managers and analysts. EL4FMS also supports users' business operations by providing access via FPNG to various financial documents relating to their FPNG account.

FEDMT: FEDMT is a database/user interface solution utilizing the Oracle Application Express (APEX) product to build small applications to support Financial Reference data as well as financial administrative tasks.

e) The way the system operates to achieve the purpose

IDP provide users access to USPTO financial-related documents to support the decision-making activities of managers and analysts. The system provides an interface for users to access the database, generate reports and ability to visualize the data.

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

The types of information collected, maintained, used, or disseminated by the system include public users' names, street addresses, e-mail addresses, and telephone numbers, gender, age, race/ethnicity, date of birth, social security number.

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

Individuals who have access to information on the system are authorized USPTO personnel requiring access the database to visualize data and generate reports in order to assist in decision-making across USPTO.

h) How information in the system is retrieved by the user

Information is retrieved via the Financial Enterprise Data Management Tools interface.

i) How information is transmitted to and from the system

Communications utilize a minimum of TLS 1.1 with FIPS 140-2 compliant algorithms to provide transmission confidentiality and integrity for all connections outside the system boundary. The externally-facing VIPs supporting IDP that exist are configured to only support TLS 1.1 and TLS 1.2.

Questionnaire:

1. 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 (version 01-2015). *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 (version 01-2017 or later). *Skip questions and complete certification.*

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 personally identifiable information (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
- ☐ National Institute of Standards and Technology Associates
- ☐ 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.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☐ No, the IT system does not collect, maintain, or disseminate SSNs, user ID is the only PII collected, maintained, or disseminated by the IT system.

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 approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Information Delivery Product and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the Information Delivery Product and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): **Gita Zoks**

Signature of SO: Users, Moore, Darrell S. (Steve) Digitally signed by Users, Moore, Darrell S. (Steve) Date: 2020.06.19 17:07:21 -04'00' Date: _____

Name of Privacy Act Officer (PAO): **John Heaton**

Signature of PAO: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2020.06.17 14:55:16 -04'00' Date: _____

Name of Chief Information Security Officer (CISO): **Don Watson**

Signature of CISO: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2020.06.22 09:27:00 -04'00' Date: _____

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): **Henry J. Holcombe**

Signature of AO & BCPO: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2020.06.25 10:30:02 -04'00' Date: _____

Name of Authorizing Official (AO) or Designated Representative: **Jay Hoffman**

Signature of AO: Users, Hoffman, Dennis (Jay) Digitally signed by Users, Hoffman, Dennis (Jay) Date: 2020.06.30 09:17:49 -04'00' Date: _____