

**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 (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).

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).

Enterprise Data Warehouse (EDW)

The Enterprise Data Warehouse (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.

Data

- EDW collects data from 20+ source systems including internal USPTO systems as well as external systems and organizes that data into five major subject areas: Financials, Revenue, Human Resources, IT Project Information, and Patents.
- EDW grants permissions to data sets, individual rows and/or individual columns of data.
- EDW delivers data to 15+ consuming systems aiding them with authoritative reference or financial data in support of their transactional data processing.

Tools

- EDW offers a secure reporting platform within SAP Business Objects, which currently hosts 1600+ individual reports including official financial reports as well as ad-hoc custom reports developed by everyday users taking advantage of EDW’s

self-service environment.

- EDW offers a secure visualization-hosting platform for Tableau visualizations sourcing data from EDW as well as those sourcing data from outside EDW.
- EDW has 75+ distinct Extract, Transform, and Load (ETL) jobs developed under SAP Data Services running at intervals of 1, 3, 5, 15, 60 minutes, or once daily, weekly, biweekly, monthly, quarterly, or annually performing approximately 200,000 loads of data every month.
- EDW offers the Enterprise Information Portal (EIP) consisting of a user interface that organizes all reports and visualizations as well as documents from our partner content management repository (EL4FMS) into a single, easy to access location.

Electronic Library for Financial Management System (EL4FMS)

The Electronic Library for Financial Management Systems (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.

Financial Enterprise Data Management Tools (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.

FEDMT currently has eight applications.

PPA Code Database to house PPA (Program, Project, and Activity) code data that previously existed in two standalone Microsoft Access databases, each separately maintained by OCIO FRMD and OCFO ABID. Both existing Access databases contained a complete listing of PPA codes; the differentiator is the OCIO database contained additional project-related attributes of interest to FRMD, and the ABID version was utilized as the official source to deliver PPA content to Momentum for financial purposes. The new APEX database serves the need of both OCFO and OCIO and contains additional attributes needed by FRMD.

EDW Security App allows EDW support personnel to administer the privileges approved for end users. Usage is limited to EDW personnel only.

IDP Admin App is utilized by EDW support staff in OFMS to create/manage content in standard reference or mapping tables, some associated with the EDW Enterprise Information Portal (EIP).

Access Request Management system (ARMS) allows users of financial systems to request access at a detailed system/role level, have those requests proceed through workflow approval processes, and alert system administrators when requests are approved and ready to implement.

Technology Business Management (TBM) app allows users in OFMS and FRMD to administer mappings of TBM data to financial reference data sets to integrate into broader reporting needs

later within the EDW and other systems.

Product Management Console (PMC) aids product management staff in the recording of Key Performance Indicators and their results, as well as provide other product management reference content and mappings to support Rally and GEARS data integration within EDW.

IT Budget Formulation Tool (ITBFT) aids the Enterprise Budget Tool (EBT) by creating a user interface for IT Product Owners to create and update budget formulation requests during open periods.

Procurement Plan (PROC) will aid procurement personnel with planning, as well as managing vendor rate data.

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

Information Delivery Product (IDP) is a Major Application.

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, used, 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 v1.2 with FIPS 140-2 compliant algorithms to provide transmission confidentiality and integrity for all connections outside the system boundary.

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	<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. *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 or 01-2017). *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 01-2019 or later). *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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
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.

IDP maintains Social Security Numbers (SSNs) of USPTO employees for human resources reporting purposes. The source systems from which it receives SSNs are the U.S Department of Agriculture (USDA) National Finance Center (NFC) and the USPTO Patent Capture and Application Processing System– Examination Support (PCAPS-ES) Patent Application Location Monitoring (PALM) Infrastructure System (INFRA).

Provide the legal authority which permits the collection of SSNs, including truncated form.

The authority for the USPTO employees' PII in IDP is E.O. 9397.

- 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

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

<p>System Owner Name: Kevin Donahoe Office: Office of the Chief Financial Officer (CFO) Phone: (571) 272-5123 Email: Kevin.Donahoe@uspto.gov</p> <p style="text-align: right; margin-right: 50px;">Users, Donahoe, Digitally signed by Users, Donahoe, Kevin Date: 2021.07.08 18:19:18 -04'00'</p> <p>Signature: <u>Kevin</u></p> <p>Date signed: _____</p>	<p>Chief Information Security Officer Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov</p> <p style="text-align: right; margin-right: 50px;">DON R Watson Digitally signed by DON R Watson Date: 2021.07.12 06:57:31 -04'00'</p> <p>Signature: <u>DON R Watson</u></p> <p>Date signed: _____</p>
<p>Privacy Act Officer Name: John Heaton Office: Office of General Law (O/GL) Phone: (571) 270-7420 Email: Ricou.Heaton@upsto.gov</p> <p style="text-align: right; margin-right: 50px;">Users, Heaton, John Digitally signed by Users, Heaton, John (Ricou) Date: 2021.07.08 16:20:07 -04'00'</p> <p>Signature: <u>(Ricou)</u></p> <p>Date signed: _____</p>	<p>Bureau Chief Privacy Officer and Co-Authorizing Official Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov</p> <p style="text-align: right; margin-right: 50px;">Users, Holcombe, Digitally signed by Users, Holcombe, Henry Date: 2021.07.12 14:39:19 -04'00'</p> <p>Signature: <u>Henry</u></p> <p>Date signed: _____</p>
<p>Co-Authorizing Official Name: Dennis J. Hoffman Office: Office of the Chief Financial Officer (CFO) Phone: (571) 272-9200 Email: Jay.Hoffman@uspto.gov</p> <p style="text-align: right; margin-right: 50px;">Users, Hoffman, Digitally signed by Users, Hoffman, Dennis (Jay) Date: 2021.07.15 14:48:53 -04'00'</p> <p>Signature: <u>Dennis (Jay)</u></p> <p>Date signed: _____</p>	