Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Master Data Management (MDM)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Master Data Management (MDM)

Unique Project Identifier: EBPL-DA-02-00

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).

The Master Data Management (MDM) system is comprised of a FedRAMP authorized Software as a Service (SaaS) suite, Collibra Data Intelligence Cloud (CDIC) and Jobserver. CDIC is a platform in which USPTO internal users can build their own data governance management system. This platform includes user management, privilege management, data catalog, workflows, and data stewardship. The CDIC platform ingests metadata, and authorized users are responsible for managing and controlling the permission and policies surrounding the data. The tool allows users to store and track metadata, create dashboards, create a business glossary, capture an inventory of reports, and use workflows to manage their data. Jobserver executes processes collecting data source meta-data which is transmitted to the CDIC Software as a Solution (SaaS) system.

Address the following elements:

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

MDM is a FedRAMP authorized SaaS system.

b) *System location*

- CDIC: This component is a SaaS suite of the tools that resides in the cloud.
- Jobserver: This executes processes collecting data source meta-data which is transmitted to the CDIC Software as a Solution (SaaS) system and is installed on servers located in the data center at 600 Dulany Street, Alexandria, VA. This server resides on the USPTO network (PTONet).

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

Systems that interconnect to MDM:

PTO-CFS Consolidated Financial System (PTOC-001-00) (CFS): CFS is a master system composed of the following four subsystems: Momentum, Concur Integration, E-Acquisition (ACQ), and VendorPortal. Momentum is a full-featured Commercial off-the-shelf (COTS) accounting software package that permits full integration of the processing of financial transactions with other normal business processes. Concur Integration works with Momentum and passes data back and forth between the systems using web services. ACQ provides an automated solution for the procure-to-pay process in the acquisition community at the USPTO. VendorPortal provides a platform for vendor interaction whereby USPTO may publish notices, solicitations and award announcements, etc.

PTO-FPNG Fee Processing Next Generation (PTOC-004-00) (FPNG): Fee Processing Next Generation is the United States Patent and Trademark Office's (USPTO) "Next Gen" solution for fee processing. FPNG allows internal and external users to manipulate payment accounts, perform profile updates, and make payments for USPTO goods and services. It also provides all functionality related to managing payments, replenishing and transferring of deposit account balances, etc. (primarily handled by the General Ledger/Account Commercial off the Shelf (COTS) Support tier/Momentum). FPNG also supports pricing rules management as well as refund requests and approvals. FPNG has interfaces to various USPTO systems and with the United States Treasury. USPTO system interfaces include MyUSPTO, Role Based Access Control (RBAC) system, Patent Application Location Monitoring (PALM), Momentum, Active Directory, Electronic Library for Financial Management Systems (EL4FMS) and the Enterprise Data Warehouse (EDW). FPNG interfaces to US Treasury include Pay.Gov and Over the Counter (OTCnet) application services.

PTO-IDP Information Delivery Product (PTOC-003-00) (IDP): IDP is a master system composed of the following three subsystems: Enterprise Data Warehouse (EDW), Electronic Library for Financial Management System (EL4FMS), and Financial Enterprise Data Management Tools (FEDMT). EDW provides a tool that allows managers and analysts to analyze business processes, resource use and needs, and other facets of the business. EL4FMS provides access to USPTO financial-related documents to support the decision-making activities of managers and analysts. FEDMT is a database/user interface solution utilizing the Oracle APEX product to build small applications to support Financial Reference data.

PTO-PBP Planning and Budgeting Products (PTOC-030-00) (PBP): PBP is a master system composed of following three subsystems: Activity Based Information System (ABIS), Analytics and Financial Forecasting (AFF), and Enterprise Budgeting Tool (EBT). ABIS streamlines and automates business processes. AFF supports the analysis of fee collection information and decision-making. EBT supports central planning and budgeting.

d) *The purpose that the system is designed to serve*

The purpose of the MDM system is to serve as a foundational tool in the effort to mature the data management practices under the Enterprise Data as an Asset initiative. It will provide USPTO internal users the following major capabilities:

- Data Catalog - Discover and understand the data that matter and allow generating insights that drive business value
- Data Governance - Establish a shared business language and understand the everevolving data landscape
- Data Lineage - Show how data flows from system to system, with complete, end-to-end lineage visualization
- Data Privacy - Operationalize and manage policies across the privacy life cycle and scale compliance across new regulations
- Data Quality – Auto-generate data quality rules to continuously improve trust in our data and analytics

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

MDM system utilizes a job server that resides on premise to connect to source databases that are cataloged within the CDIC. It runs jobs to collect metadata from the data sources and transmits the metadata to CDIC. This provides USPTO users with an enterprise-oriented data governance platform for data governance and stewardship. USPTO users are able to better analyze their data, improve business decisions, and business and IT can collaborate.

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

MDM system will ingest metadata on USPTO source databases. This includes information that will allow it to perform data catalog, data lineage, data governance, and data privacy capabilities. This includes data classification, mapping, dictionary, and profiling information.

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

MDM allows internal user access (i.e. DOC employees and contractors working on behalf of DOC).

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

MDM allows users to retrieve information in electronic format. MDM allows user access to the CDIC platform, where they can perform contextual search and access reports and dashboards.

i) How information is transmitted to and from the system

MDM transmits metadata to CDIC cloud using a secured HTTPS connection.

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

☒ 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 Master Data Management (MDM) 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 Master Data Management (MDM) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Kevin Donahoe Office: Office of the Chief Financial Officer (OCFO) Phone: (571) 272-5123 Email: Kevin.Donahoe@uspto.gov Signature: Users, Donahoe, Kevin Digitally signed by Users, Donahoe, Kevin Date: 2023.04.18 12:33:09 -04'00' 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: 2023.05.01 12:28:22 -04'00' Date signed: ______________________________
Privacy Act Officer Name: Kyu Lee Office: Office of General Law (O/GL) Phone: (571) 272-6421 Email: Kyu.Lee@uspto.gov Signature: Users, Lee, Kyu S. Digitally signed by Users, Lee, Kyu S. Date: 2023.04.24 18:58:28 -04'00' Date signed: ______________________________	**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 Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.05.02 11:44:35 -04'00' Date signed: ______________________________
Co-Authorizing Official Name: Jay Hoffman Office: Office of the Chief Financial Officer (OCFO) Phone: (571) 272-7262 Email: Jay.Hoffman@uspto.gov Signature: Users, Hoffman, Dennis (Jay) Digitally signed by Users, Hoffman, Dennis (Jay) Date: 2023.05.04 15:50:12 -04'00' Date signed: ______________________________	