Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Master Data Management (MDM)

Reviewed by: Henry J. Holcombe, 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

JENNIFER GOODE Digitally signed by JENNIFER GOODE Date: 2022.03.25 11:15:20 -04'00' 3/25/2022

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO Master Data Management (MDM)

Unique Project Identifier: EBPL-DA-02-00

Introduction: System Description

Provide a brief description of the information system.

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
The locations of the MDM components are as follows:

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

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 ever-evolving 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) 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.

(f) How information is transmitted to and from the system

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

(g) Any information sharing

MDM collects information about USPTO employees and contractors such as First Name, Last Name, and Email Address. This information is based on roles associated with various data domains (e.g., Name of the Data Owner role of the Patent Quality Data) and will be shared within the bureau on a case-by-case basis.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The following federal laws provide the specific programmatic authority for collecting, maintaining, using, and disseminating the information: E-Government Act of 2002; and Foundations for Evidence-Based Policymaking.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

The FIPS 199 security impact category for MDM is 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):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

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. Gender	☐	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):					

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):					

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):					

2.3 Describe how the accuracy of the information in the system is ensured.

MDM is secured using appropriate administrative, physical and technical safeguards in accordance with the NIST security controls (encryption, access control, auditing). Mandatory IT Awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose of data. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data.

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.
☒	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):			

☒	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).

The information in this system is about USPTO employees and contractors and is used for administrative matters and to promote information sharing initiatives. By providing an enterprise-oriented data governance platform for data governance and stewardship, USPTO users are able to better analyze their data, improve business decisions, and allow for better collaboration between business units and the and IT departments.

The information collected is primarily used for administrative purposes. For example, Work Email Address is used for notification emails to notify users of any changes made to assets; IP Address and Date/Time of Access are used for logging and auditing purposes.

MDM to serve as a foundational tool in the effort to mature the data management practices under the Enterprise Data as an Asset initiative.

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 from USPTO employees or contractors stored within the system could be exposed, the USPTO has policies, procedures and training to ensure that employees are aware of their responsibility of protecting sensitive information and the negative impact on the agency if there is a loss, misuse, or unauthorized access to or modification of sensitive private information. Physical access to servers is restricted to only a few authorized individuals. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIOPOL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). 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: MDM receives information, system and application logs) from the following other USPTO systems that have been authorized to process PII and or BII: • CFS • IDP • FPNG • PBP The technical controls in place to prevent PII/BII leakage include encryption, antivirus and antimalware, firewalls, SIEM, Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS). Access to PTO data is via a VPN and Privilege access controls are maintained via Active directory. services are logically partitioned via a DMZ and an internal USPTO firewall is used as the boundary protection device that secures the communication between internet users and the systems they access. The Data within MDM is also secured via FedRAMP-authorized Collibra - Collibra Data Intelligence Cloud (CDIC), and established controls to include password authentication at the server levels. HTTPS is used for all data transmissions to and from the Internet and PTONet.
☐	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: http://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: See Appendix A
☐	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: Users of USPTO systems receive a warning banner notification regarding consent to be monitored by using the system and therefore do not have the opportunity to decline to provide PII/BII.

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: MDM data is used to provide users access to the system. Data is also collected via system monitoring in the form of audit logs. Because the data is used to allow users to access the system and the nature of how the audit data is collected, users do not have the opportunity to consent to particular uses of their PII/BII.

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	Specify how: USPTO employees and contractors have the opportunity to review/update their PII with office of Human

	them.	resources.
☐	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): _____ ☒ 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 4 Appendix J 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).*

MDM is secured by the USPTO's infrastructure systems, FedRAMP-authorized Collibra - Collibra Data Intelligence Cloud (CDIC), and established controls to include password authentication at the server levels. HTTPS is used for all data transmissions to and from the Internet and PTOnet.

Management Controls:
The USPTO uses the Life Cycle review process to ensure that management controls are in place for the MDM. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the Security Plan. The Security Plans specifically address the management, operational, and technical controls that are in place, and planned during the operation of the enhanced system. Additional management controls include performing national agency check on all personnel, including contractor staff.

Operational Controls: Operational controls include securing all hardware associated with this system in the USPTO Data Center. The Data Center is controlled by access card entry, and manned by a uniformed guard service to restrict access to the servers, their operation systems and databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions" (2) Physical terminal identification; (3) Database UserID; (4) restricted data display, as required; and (5) restricted access. Technical Controls: Technical controls include password authentication (UserID and passwords). At the client PCs', access is managed through a password authentication (UserID and passwords) based on certification in Access Request Management System (ARMS). Requests are approved first by the user's supervisor based on a justification of need.

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)*: Commerce/Dept 18: Employees Personnel Files Not Covered by Notices of Other Agencies. Commerce/PAT-TM-17: USPTO Security Access Control and Certificate Systems.
☐	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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule:

	GRS 3.1, item 010, Information technology development project records; Infrastructure project records. GRS 3.1, item 011, Information technology development project records; System development records. GRS 3.1, item 012, Information technology development project records; Special purpose computer programs and applications. GRS 3.1, Item 040, Information technology oversight and compliance records. GRS 5.2, item 020, Intermediary records. GRS 6.3, item 010, Information Technology program and capital investment planning records. GRS 6.3, item 020, Enterprise architecture records.
☐	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: The information such as name, work email address, and User ID captured by the MDM system could identify an individual.
☒	Quantity of PII	Provide explanation: MDM will collect data from a small segment of internal users for purposes of account set up. Also,

		there is the potential for PII data to be included over time within the logs collected by the system.
☒	Data Field Sensitivity	Provide explanation: The combination of name, user ID and email address have a low impact on the date field sensitivity.
☒	Context of Use	Provide explanation: MDM data is account data that will be used by a select segment of internal users who will access the system.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected, USPTO must protect the PII of each individual in accordance with the Privacy Act of 1974 which prohibits the disclosure of information from a system of records absent of the written consent of the subject individual.
☒	Access to and Location of PII	Provide explanation: Access Control Lists limits access to MDM to only a few approved authorized accounts. Authorized privileged users access the applications for administrative functions only, and authorized non-privileged users access some applications as required for their roles within their group. The servers storing the potential PII are located in a highly sensitive zone within the USPTO internal network and logical access is segregated with network firewalls and switches.
☐	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.)

Access to MDM is very limited and controlled by the MDM PM team. IDM accounts must be created by Operations for new accounts requested by members of the MDM PM team. Data is protected in transit through TLS 1.2. Administrative access to the back-end on premise servers is limited to trusted individuals on the development team. Given the limited access under this category, the threat of PII leakage is very low but can be a potential threat to privacy. Access to the user interface is not exposed to the public internet and only accessed within the USPTO network.

USPTO has identified and evaluated potential threats to PII such as loss of confidentiality and integrity of information. Based upon USPTO's threat assessment policies, procedures, and training has been implemented to ensure that employees are aware of their responsibility to protect PII and to be aware of insider threats. Our employees are aware of the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of PII.

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.

APPENDIX A

You are accessing a U.S. Government information system, which includes: 1) this computer, 2) this computer network, 3) all Government-furnished computers connected to this network, and 4) all Government-furnished devices and storage media attached to this network or to a computer on this network. You understand and consent to the following: you may access this information system for authorized use only; unauthorized use of the system is prohibited and subject to criminal and civil penalties; you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system at any time and for any lawful Government purpose, the Government may monitor, intercept, audit, and search and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. This information system may contain Controlled Unclassified Information (CUI) that is subject to safeguarding or dissemination controls in accordance with law, regulation, or Government-wide policy. Accessing and using this system indicate your understanding of this warning.