Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Information Delivery Product (IDP)

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2023.08.01 12:00:40 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Information Delivery Product (IDP)

Unique Project Identifier: PTOC-003-00

Introduction: System Description

Provide a brief description of the information system.

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.

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. There are no Personally Identifiable Information and no Business Identifiable Information.

Address the following elements:

(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*
On premise components reside at the USPTO facilities located in Manassas, Virginia Cloud components are housed within Amazon Web Services (AWS).

(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:

The Agency Administrative Support System (AASS) is an application information system that works to consolidate imaging document system within the Corporate System Division (CSD) and enable USPTO to manage and track automated hardware and software assets from the time of their acquisition to retirement.

Corporate Administrative Office System (CAOS) is an application information system. The purpose of the CAOS is to support the Human Resources business functions within the United States Patent and Trademark Office (USPTO).

Consolidated Financial System (CFS) is a Master System composed of the following four (4) subsystems: 1) Momentum, 2) Concur Integration, 3) E-Acquisition (ACQ), and 4) VendorPortal.

Corporate Web Systems (CWS) provides a feature-rich and stable platform that contains the Organizations Websites that are used at USPTO such as Intranet and USPTO external website.

Enterprise Desktop Platform (EDP) is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 7 and Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

Enterprise Records Management and Data Quality System (ERMDQS) is a Major Application (MA) consisting of one Automated Information Systems (AIS): Data Architecture Tool – Metadata (DAT-Metadata). Data Architecture Tool – Metadata (DAT-Metadata) is a central source of information for the entire USPTO.

Enterprise Software Services (ESS) system provides an architecture capable supporting current software service as well as provide the necessary architecture to support the growth anticipated over the next five years.

Enterprise UNIX Services (EUS) is an infrastructure operating system with a sole purpose of providing a UNIX base hosting platform to support other systems at USPTO.

Enterprise Windows Servers (EWS) EWS is an Infrastructure information system which provides a hosting platform for major applications that support various USPTO missions.

Fee Processing Next Generation program (FPNG) will replace the RAM system with 21st Century Technologies and implement flexibility to quickly change business rules and other configuration changes without requiring code changes.

Network and Security Infrastructure System (NSI) The NSI facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

Patent Capture and Application Processing System (PCAPS-ES): The purpose of this system is to process, transmit and store data, and images to support the data-capture and conversion requirements of the USPTO to support the USPTO patent application process.

Patent Trial and Appeal Board End to End (PTAB E2E). The purpose of the PE2E is to provide examination tools for Central examination unit to track and manage the cases in this group and view documents in text format.

Service Oriented Infrastructure (SOI) provides a feature-rich and stable platform upon which USPTO applications can be deployed.

USPTO Amazon Cloud Services (UACS) - The UACS General Support System is a standard infrastructure platform that supports USPTO Application Information Systems (AIS) hosted in Amazon Web Services (AWS).

(d) The way the system operates to achieve the purpose(s) identified in Section 4
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.

(e) How information in the system is retrieved by the user
Information is retrieved via the Financial Enterprise Data Management Tools interface.

(f) How information is transmitted to and from the system
Communications utilize a minimum of Transport Layer Security (TLS) v1.2 with FIPS 140-2 compliant algorithms to provide transmission confidentiality and integrity for all connections outside the system boundary.

(g) Any information sharing
IDP supports users' business operations by providing access via FPNG to various

financial documents relating to their FPNG account.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
The USPTO collects customer financial information for fee processing under 35 U.S.C. 2 and 41 and 15 U.S.C.1113, as implemented in 37 CFR 1.16–1.28, 2.6–2.7, and 2.206–2.209. The authority for the USPTO employees' PII in IDP is E.O. 9397.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
IDP is categorized as a Moderate system.

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: 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).					

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.

Data is pulled from PTO authoritative sources which have the responsibility for data accuracy. USPTO implements security and management controls to prevent the inappropriate disclosure of sensitive information. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and expected by authorized users. Management controls are utilized to prevent the inappropriate disclosure of sensitive information. Access controls, including the concept of least privilege, are in place within the system to protect the integrity of this data as it is processed or stored. IDP receives PII/BII indirectly from other application systems which are responsible for enabling users to update their information and ensure accuracy.

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.

	0651-0043 Financial Transactions
☐	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): Click or tap here to enter text.			

☒	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 Delivery Product integrates existing data from multiple USPTO sources and HR data from the U.S Department of Agriculture (USDA) National Finance Center (NFC). It makes data comparisons available for analysis. This systems collects, maintains, or disseminates information about DOC employees, Contractors (working for DOC), and Members of the Public.

This information is collected to support the decision-making activities of managers and analysts in the PTO's business areas to analyze USPTO data. Specifically, the information will provide managers and analysts the ability to analyze business processes, resource use and needs, and other facets of the business and provide the USPTO with the means of performing at a more efficient, accurate, and cost effective level.

One subject area of the IDP is the Human Resources Subject Area (HRSA). HRSA is a reporting mechanism for HR to allow authorized users (both within OHR and for managers throughout PTO) to run reports, such as staff listings, within Grade Increases projections, employee counts, accession/separation lists, etc. The data warehouse (which stores USDA NFC, U.S Treasury HR Connect, and general employee locator content) in conjunction with the Business objects reporting tool, allows for the dissemination of information to authorized users.

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.)

The potential danger in the PII/BII being compromised is the potential for sharing of information that is required to be held in confidence for a specified period of time per statute and regulation, e.g., 35 USC 122 and 37 CFR 1.211. Adversarial entities, insider threats, and foreign governments can be potential threats to privacy. All end-users and administrators of the BDR system have a valid need-to-know access to the system, and undergo the USPTO Annual IT Security Awareness Training provided by the agency. This training covers proper information handling, retention, and disposal at an enterprise level, which is applicable to all information systems.

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: Agency Administrative Support System (AASS) Consolidated Financial System (CFS) Corporate Administrative Office System (CAOS) Corporate Web Systems (CWS) Enterprise Desktop Platform (EDP) Enterprise Software Services (ESS) Enterprise UNIX Services (EUS) Enterprise Windows Servers (EWS) Fee Processing Next Generation program (FPNG) Network and Security Infrastructure System (NSI) Patent Capture and Application Processing System (PCAPS-ES)

	Patent Trial and Appeal Board End to End (PTAB E2E) SOI (Service Oriented Infrastructure) The information transmitted between the systems is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) system. All data transmissions are encrypted and require credential verification. All data transmissions not done through dedicated lines require security certificates. Inbound transmissions as well as outbound transmissions to government agencies pass through a DMZ before being sent to endpoint servers. SSNs and Taxpayer IDs are encrypted while at rest.
☐	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: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). Individuals may be notified that their PII/BII is collected, maintained, disseminated by the primary application ingress system.
☐	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: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). These front end systems provide this functionality for the data that is being collected. IDP has no authorization to decline any type of information since it's owned by the primary application

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: IDP receives PII/BII indirectly from application systems (i.e front end systems). These front end systems provide this functionality for data that is being collected. USPTO Employees and Contractors do not have the ability to consent to particular uses of their PII. They consent to providing their name, SSN, and phone number etc. as part of accepting employment at USPTO.

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 them.	Specify how:
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: IDP receives PII/BII indirectly from other application systems (i.e. front end systems). These front end systems provide this functionality for the data that is being collected. IDP has no authorization to review/update any type of information since it's owned by the primary application.

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: The EDW system has implemented logging, auditing, and monitoring tools to track access to PII/BII.
☒	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): 8/29/2022 ☐ 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).*

Management Controls:
The USPTO uses the Life Cycle review process to ensure that management controls are in place for the IDP. 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 User ID; (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 a Financial Access Request Management (FARM) system. Requests are approved first by the user's supervisor, then requires additional approval from Human Resources based on a justification of need. 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 on a Financial Application Security Registration form. The security form must be signed by a supervisor, and requires additional approval from Human Resources 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)*: Existing System of Records notices cover the information pulled from other systems residing in the Enterprise Data Warehouse. These include: Commerce/PAT-TM 3, Employee Production records; Commerce/PAT-TM-7, Patent Application Files; Commerce/PAT-TM 10, Patent Deposit Accounts System; and Commerce/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies
☐	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 4:3:031 records schedule
☐	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: Social Security Number (SSN), name, gender, age, race/ethnicity, home/business address, email address, telephone number, financial information all of these factors can be used to identify a person.
☒	Quantity of PII	Provide explanation: Collectively, the number of records maintained generate an enormous amount of PII and a breach in such large numbers of individual PII must be considered in the determination of the impact level.
☒	Data Field Sensitivity	Provide explanation: Combination of name, SSN, and financial information may be more sensitive.
☒	Context of Use	Provide explanation: PII is stored to support the decision making activities of managers and analysts in the PTO's business areas to analyze USPTO data.
☒	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected, USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: Due to obtaining PII, necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission.
☐	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.)

IDP resides in USPTO East production environment. Access to IDP is very limited and controlled by the IDP PM team. IDM accounts must be created by Operations for new accounts requested by members of the IDP PM team. Data is protected in transit through TLS1.2. Administrative access to the back-end is limited to trusted individuals on the development team. Access to the IDP is controlled through RBAC enforcement. The correspondence related to non-published applications are made public when the application is made public (typically after a period of 18 months). Given the limited access under this category, the threat of BII 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 kept internally within the USPTO network.

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.

Points of Contact and Signatures

System Owner
Name: Kevin Donahoe
Office: Office of the Chief Financial Officer (CFO)
Phone: (571) 272-5123
Email: Kevin.Donahoe@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Donahoe, Kevin Digitally signed by Users, Donahoe, Kevin Date: 2023.07.10 18:28:29 -04'00'

Date signed: _____

Chief Information Security Officer
Name: Timothy S. Goodwin
Office: Office of the Chief Information Officer (OCIO)
Phone: (571) 272-0653
Email: Timothy.Goodwin@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: _____ Digitally signed by Timothy Goodwin Date: 2023.07.24 08:42:43 -04'00'

Date signed: _____

Privacy Act Officer
Name: Ezequiel Berdichevsky
Office: Office of General Law (O/GL)
Phone: (571) 270-1557
Email: Ezequiel.Berdichevsky@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2023.07.20 17:21:04 -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

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.08.01 12:02:26 -04'00'

Signature: Users, Stephens, Deborah Digitally signed by Users, Stephens, Deborah Date: 2023.07.28 12:25:51 -04'00'

Date signed: _____

Co-Authorizing Official
Name: Jay Hoffman
Office: Office of the Chief Financial Officer (OCFO)
Phone: (571) 272-9200
Email: Jay.Hoffman@uspto.gov

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: Users, Hoffman, Dennis (Jay) Digitally signed by Users, Hoffman, Dennis (Jay) Date: 2023.08.07 09:38:11 -04'00'

Date signed: _____

This page is for internal routing purposes and documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.