Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Enterprise Data Service System -Databricks (EDS-DBX)

Reviewed by: Deborah Stephens, 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

TIFFANY DANIEL Digitally signed by TIFFANY DANIEL
Date: 2026.04.21 09:09:32 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Enterprise Data Service System -Databricks (EDS-DBX)

Unique Project Identifier: EBPL-DA-03-00

Introduction: System Description

Provide a brief description of the information system.

The Enterprise Data Service System – Databricks (EDS-DBX) is a data analysis platform that helps the United States Patent and Trademark Office (USPTO) gain valuable insights from large volumes of data. The system supports data-driven decision-making by enabling advanced analytics, performance and quality management, and the use of technologies for distributed computing.

EDS-DBX provides USPTO data scientists, engineers, and analysts with a unified workspace where they can securely explore, process, and analyze data to support agency operations and research related to improving federal services online and supporting USPTO human resources administration through employee performance measurements. The platform allows for both interactive exploration and scheduled analysis of USPTO datasets. In addition, system administrators and technical leads have controlled access to manage user permissions and oversee system operations, ensuring that data is handled responsibly and securely. Language related to Artificial Intelligence and machine learning (AI/ML) were removed from the PIA because the data and compute capabilities are performed in the respective interconnected systems.

Address the following elements:

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

Major Application

(b) System location

The application is hosted in Alexandria, VA

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

EDS-DBX is interconnected with:

Open Data Big Data Master System (ODBD-MS) – This system includes Internal Data Hub (IDH) – a centralized platform that provides the infrastructure and tools needed to support advanced analytics across the USPTO. IDH brings together multiple data sources, hosted within USPTO AWS cloud services (UACS) to create statistical models and visualizations that help the agency analyze trends, improve performance, and support strategic decision-making. EDS-DBX provides SaaS services to this system and may access the data periodically to check for the status of various services which may include EDS-DBX receiving PII from this system

Information Delivery Product (IDP) – This system is a collection of components and tools sharing analytic and data themes used in the production of business intelligence and advanced analytical solutions as well as services for designing and developing those solutions. EDS-DBX provides SaaS services to this system and may access the data periodically to check for the status of various services which may include EDS-DBX receiving PII from this system.

ICAM Identity as a Service (ICAM-IDaaS) – This system includes the monitoring, support, management, and operations support services for the enterprise and includes the IT Service Management (ITSM) functions. EDS-DBX provides SaaS services to this system and may access the data periodically to check for the status of various services which may include EDS-DBX receiving PII from this system.

Security and Compliance Services (SCS) – This application is a Security Information and Event Manager (SIEM) system that collects and consolidates USPTO Information System event log data from all USPTO hosts and devices configured to send their audit log files to the SIEM QRadar collector devices. The SIEM system collects network infrastructure, net-flow data to use in conjunction with operating system and hardware log data that it collects and stores. The SIEM system maintains separate data and correlates events to share with the EMS system to produce actionable, real-time alerts and around the clock monitoring in detailed display. EDS-DBX pushes log and audit data generated within its SaaS services to this system.

M365-M365 INTERNAL (M-365) – Enabling all USPTO internal users' ability to perform work in support of the USPTOs mission of awarding qualified U.S. patents and registering qualified trademarks in a timely and cost-effective manner. EDS-DBX provides SaaS services to this system and may access the data periodically to check for the status of various services which may include EDS-DBX receiving PII from this system. EDS-DBX interfaces with M-365 to send updates/monitoring emails related to various SaaS services to admins and users.

International Data Exchange (IDE) – Users products and services that allows access to and retrieval of Patent Classifications and related work sharing events**.** EDS-DBX provides SaaS

services to this system and may access the data periodically to check for the status of various services which may include EDS-DBX receiving PII from this system

Trademark Common Services (TM-CMC-C) – This system is collection of data pipelines and data stores consolidating data from Trademark operational systems into the enterprise data and analytics product affording the creation of crucial datasets supporting desired Trademark as well as USPTO business intelligence and analytics. EDS-DBX provides SaaS services to this system and may access the data periodically to check for the status of various services which may include EDS-DBX receiving PII from this system.

Patent Business Management Information – Cloud (PBMI-C) – This system is collection of data pipelines and data stores consolidating data from Patent operational systems within the Patent Product Line to the Patent Business Management Information product affording the availability and governance of crucial datasets supporting desired Patents as well as USPTO business intelligence and analytics. EDS-DBX provides SaaS services to this system and may access the data periodically to check for the status of various services which may include EDS-DBX receiving PII from this system.

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

EDS-DBX only provides control to the compute and data that happens in the various interconnected systems. Databricks works by using logic to parse information from large datasets spread across different products/sources to analyze and derive an output. The initial data is ingested as is, by the interconnected systems and stored in their USPTO AWS Cloud Services (UACS) accounts and processed using data engineering, analytics, data science to generate result data. The output is sent to a specified UACS location of the interconnected system by invoking a Databricks job every time a batch of data is ready to be processed.

(e) How information in the system is retrieved by the user

Transfer of data into EDS-DBX for processing is done using a private link between each connecting system. Users retrieve information through multiple interfaces tailored to different roles and technical expertise. Interactive notebooks support SQL, Python, Scala, and R for data exploration and analysis, while Databricks SQL provides a web-based query editor and dashboards for business analysts requiring no coding skills. Technical users access data programmatically via REST APIs, JDBC/ODBC connections, or the Databricks CLI, enabling integration with BI tool like Tableau.

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

The information is transmitted using TLS 1.3 via bulk data transfer from interconnected systems internal to USPTO.

(g) Any information sharing

Only administrators have access to the data in the application, EDS-DBX is not a public facing website. The data in the application can be retrieved using scheduled jobs and SQL queries.

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

35 U.S.C. Chapter 1, 40 U.S.C. 11301 note, EO 13960, EO 14110

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

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): EDS-DBX has the capability of pulling data from its Interconnected systems (see Section C.) which can include the PII listed in this audit data.					
*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. Sex	☐	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): EDS-DBX has the capability of pulling data from its Interconnected systems (see Section C.) which can include the PII listed in this audit data.					

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): EDS-DBX has the capability of pulling data from its Interconnected systems (see Section C.) which can include the PII listed in this audit data.					

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): EDS-DBX has the capability of pulling data from its Interconnected systems (see Section C.) which can include the PII listed in this audit data.					

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): EDS-DBX has the capability of pulling data from its Interconnected systems (see Section C.) which can include the PII listed in this audit data.					

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 a USPTO authoritative sources which has the responsibility for maintaining data accuracy. The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

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. 0651-0009 Trademarks Processing 0651-0031 Initial Patent Applications
☐	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).

EDS-DBX provides SaaS services to its interconnected systems and may access the data periodically to check for the status of various services which may include EDS-DBX receiving PII from these systems. PII/BII data is ingested into the interfacing systems and crosses into EDS-DBX boundary only when using the analytics tools. This PII/BII data is never stored in the EDS-DBX system.

The PII/BII data identified in the System Administration/Audit Data (SAAD) under section 2.1 is in reference to federal employees and contractors only.

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 stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information. NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. 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: Information Delivery Product (IDP) Open Data Big Data Master System (ODBD-MS) Security and Compliance Services (SCS) M365-M365 INTERNAL (M-365) International Data Exchange (IDE) Trademark Common Services (TM-CMC-C) Patent Business Management Information – Cloud (PBMI-C) NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. 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.
☐	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 policy. The privacy `be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: This PIA serves as notice.
☐	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: Access to the EDS-DBX system is voluntary for Data scientists/engineers and Admins (federal employees and contractors).
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: Individuals do not have the opportunity to consent to participate uses of their PII/BII because the data is not directly collected from them

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: Individuals do not have the opportunity to decline providing PII because access to the EDS-DBX system is voluntary.

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): 6/23/2025 ☐ 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 5 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).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in the System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

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/PAT-TM-7 Patent Application Files COMMERCE/PAT-TM-26 Trademark Application and Registration Records
☐	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.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: Development Trademark Case File Feeder Records and Related Indexes - N1-241-06-2:4, Temporary: Destroy or delete when transfer to official Trademark Case File has been verified and the feeder documentation is no longer needed for current agency business. **3.2: Information Systems Security Records** 030-031 - System Access Records **Systems not requiring special accountability for access**. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. **Temporary.** Destroy when business use ceases. **Systems requiring special accountability for access**. These are user identification records associated with systems which are highly sensitive and potentially vulnerable.

	Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. General Technology Management Records - Information technology operations and maintenance records – GRS 3.1:020 - Including System logs – Temporary: Destroy 3 years after (See GRS for cutoff instructions).
☐	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: Records Management will need to work with the system owner, the system technical support members, and the BU stakeholders to draft a records schedule to submit to NARA fore review and approval.

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: PII data (SAAD data and Employee Name) used in EDS-DBX is related to USPTO employees and contractors.
☒	Quantity of PII	Provide explanation: Approximately hundreds of records will be

		processed on a daily basis.
☒	Data Field Sensitivity	Provide explanation: Should there be any unauthorized access, modification and/or disclosure of the PII/BII contained within this system would have a moderate impact on the organization.
☒	Context of Use	Provide explanation: The PII/BII collected will be used for system administration and security auditing.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. In accordance with the Privacy Act of 1974, PII must be protected.
☒	Access to and Location of PII	Provide explanation: The PII ingested into Databricks is stored in another Information System Security and Compliance Services (SCS).
☐	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.)

The Databricks application resides in the Amazon cloud with no access to the general public. User access is provisioned only to administrators who perform maintenance tasks, the threat of BII/PII leakage is low because the data being shared to Databricks has safeguards put in place to protect the data but if the data was to be exposed it will pose a risk to the organization.

System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified. Machine learning is checked by humans for error per EO 13960.

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.