Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
Level Access Accessibility Management Platform (AMP)

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

BRIAN ANDERSON

Digitally signed by BRIAN ANDERSON
Date: 2025.08.27 12:17:51 -04'00'

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

On behalf of Acting SAOP

U.S. Department of Commerce Privacy Impact Assessment
USPTO Level Access Accessibility Management Platform (AMP)

Unique Project Identifier: EBPL-CCX-06-00

Introduction: System Description

Provide a brief description of the information system.

Level Access Accessibility Management Platform (AMP) is a web-based platform (cloud based) that provides a solution for United States Patent and Trademark Office (USPTO) to meet Section 508, Americans with Disabilities (ADA) and Web Content Accessibility Guidelines (WCAG) compliance needs. It does this on the platform by viewing or uploading web pages and files (such as Portable Document Format (PDF's), and videos) from www.uspto.gov and USPTOs internal website (PTOWeb), then providing feedback on the AMP platform. Both www.uspto.gov and PTOWeb features newsworthy inventors, along with other pertinent information. AMP also provides best practices, as well as provides an extensive training course library.

AMP will be used only internally here at USPTO. All users of AMP will be USPTO employees or contractors. AMP uses multi-factor authentication (MFA), and is not available to the public.

AMP does not store any PDF's or web pages. It reads the data, and produces a report It does save the reports.

Address the following elements:

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

Minor Application

(b) System location

Amazon Web Services (AWS) and 1310 Courthouse Rd, Arlington, VA, 22201.

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

AMP interconnects with:

PTO-EIPL-DS-ICAM-IDaaS ICAM Identity as a Service (EIPL-DS-03-00): is an infrastructure information system that provides authentication and authorization services to secure all USPTO enterprise applications and provides auditability to user activity. The specific IDaaS in use is Okta.

PTO-EIPL-DS-ID-AUTH-Identity Management Authenticator (EIPL-DS-09-00): purpose is the personalization and issuance and management of the smart card identification credentials under Homeland Security Presidential Directive-12 (HSPD-12), issuance and management of Rivest, Shamir, Adleman (RSA) authentication tokens and issuance and management of Internet Public Key Infrastructure (IPKI) digital certificates.

PTO-EIPL-ESS Enterprise Software Services (PTOI-020-00): controls USPTO access controls such as PIV card.

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

Selected USPTO employees will login to their computer via their Personal Identity Verification (PIV) card to the USPTO network. They will then visit the USPTO AMP site (https://uspto.levelaccess.us/) click the "Login via Security Assertation Markup Language (SAML)" link and access AMP. The user can either enter a URL directly into AMP, or use their upload feature. AMP will generate a report with distinct areas that need to change to make the tested material compliant. The PDF's/webpages are not stored within the application.

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

Authorized USPTO employees and contractors retrieve information in the system by logging into the platform via ICAM-IDaaS, using SSO with SAML. This ensures secure, authenticated access to the system.

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

AMP is accessed remotely through a secure internet connection. User authentication is facilitated though a Single Sign-On (SSO) process using Security Assertion Markup Language (SAML) via Okta, which serves as the identity provider to verify user credentials and manage session tokens for federated access.

Information exchanged with the system is transmitted using a web browser over Hypertext Transfer Protocol Secure (HTTPS). HTTPS ensures confidentiality, integrity, and authentication of the data through Transport Layer Security (TLS) encryption. The protocol

initiates a secure session using a cryptographic key exchange, encrypts all transmitted data, and maintains secure communication until the session ends – protecting the data from interception or tampering throughout. . The PDF's/webpages are not stored within the application. Only the reports generated are stored within the application.

(g) Any information sharing

AMP shares information such as System Administration/Audit Data, Work-related Data, General Personal Data and Identifying Numbers via its web interface to internal USPTO employees and contractors.

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

Section 508 of the Rehabilitation Act of 1973

(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):					
*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)
All of the above information is collected because it is also available on the sites that we are testing. For example, employee's name is available on our internal intranet site, therefore, AMP will also have access to that data. The same situation applies for our external website – www.uspto.gov. If it is available on www.uspto.gov, then AMP will also have access to it (to test if it is 508 compliant). AMP also has access to some data for the minimal people that are USPTO administrators of AMP.

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):					

How is PII collected directly from individuals?

From www.uspto.gov, PII can come from interviews or biographies that are listed on www.uspto.gov. From PTOWeb (intranet), it can come from an employee directory or biographies.

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

The accuracy of the information in the system is maintained by collecting it directly from the individual who provides it, without making any modifications, The person who inputs the information into AMP can review it after it has been uploaded to ensure its accuracy. AMP 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. 0651-0077, National Summer Teacher Institute 0651-0080, Clearance for the Collection of Qualitative Feedback on Agency Service Delivery 0690-0035, Generic Clearance for Managing Customer Experience and Improving Service Delivery OMB Circular A-11, Section 280
☐	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 PII uploaded as indicated in section 2.1 could be about USPTO employees, contractors or members of the public and is used to ensure 508 compliance for documents that will be made widely available. For administrators, who are federal contractors and employees, user ID, and audit log data is collected. System users undergo annual mandatory training regarding appropriate handling of information 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.

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.)

Users who have access to the system are limited to a few USPTO employees or contractors.

The threats to privacy are insider threats, and foreign governments. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The annual training has made all employees aware of the possibility of insider threats and threats from adversarial or foreign entities and how these bad actors can affect USPTO's reputation. The following are USPTO's current policies that are adhered to: IT Privacy Policy (OCIO-POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), and USPTO Rules of the Road (OCIOPOL36). The combination of USPTO trainings and policies will help USPTO employees to recognize insider threats and threats from adversarial or foreign entities. 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.

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. 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: ICAM IDaaS ID-AUTH Enterprise Software Services 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 from the ingestion system. 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: This PIA serves as a 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: Newsworthy members of the public may decline to be featured. It is part of the USPTO process to include the biography of senior leadership. They may opt to not provide biography and/or photograph.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Administrators of the system cannot decline to have their information stored due to system audit activity.

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: Newsworthy inventors sign a consent as part of the process of creating the article. There have been hundreds (possibly thousands) of inventors that have been featured or mentioned on our websites. Senior leadership provides the content of the featured biographies of the USPTO leaders.
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals who have access AMP do not have the opportunity to consent to particular uses of their PII/BII as it is necessary for them to be granted access to AMP which is part of their USPTO responsibilities.

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 an opportunity to review / update their PII/BII directly in AMP. For Senior leaders and newsworthy innovators, they can submit requests to their point of contact to update or request corrections to their information. For individuals with access to the system, they can review some of their information within the system but would need to contact HR to get their information updated from the source system.

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 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)*: DEPT-25- Access Control and Identity Management System
☐	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: GRS 5.1, item 020 – Non-recordkeeping copies of electronic records GRS 3.1: General Technology Management Records GRS 3.2: item 035 – Cybersecurity logging records (including system logs).
☐	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: Names, telephone numbers, work email, and education can be all combined to identify an individual
☒	Quantity of PII	Provide explanation: The quantity of PII from administrators will be dependent on the amount of users, but not to exceed 50 people. The amount of PII that AMP is processing is dependent on what was published at that time on PTOWeb or www.uspto.gov
☒	Data Field Sensitivity	Provide explanation: The data includes limited personal and work-related elements and does not include sensitive identifiable information since all the information processed by AMP is public record information.
☒	Context of Use	Provide explanation: Serves as system to help our sites become more accessible to those with disabilities
☒	Obligation to Protect Confidentiality	Provide explanation: There is no obligation to protect the confidentiality of the PII, the PII processed by AMP is publicly available.
☒	Access to and Location of PII	Provide explanation: The PII within this system is available to the public. The system stores its data within the cloud and thus logical access is enforced for backend database maintenance. The PII on this system is available to the general public on the websites listed above.
☐	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 PII in this system poses a risk if exposed. 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.

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.