Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
CoSo Cloud Adobe Connect Solution (UCCACS)

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: 2024.03.12 17:47:34 -04'00' 9/20/2024

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO CoSo Cloud Adobe Connect Solution (UCCACS)

Unique Project Identifier: EIPL-EUS-03-00

<u>Introduction</u>: System Description

Provide a brief description of the information system.

USPTO CoSo Cloud Adobe Connect Solution (UCCACS) is a web communication solution that enables USPTO to provide online computer-based training to internal audiences. The purpose of this system is to enable USPTO business units to share vital knowledge with USPTO staff. USPTO business units gain efficiency and effectiveness by communication and sharing viral business knowledge with internal customers. The UCCACS system users are comprised of employees and contractors, including system administrators and regular users that access the system internally through PTONet. Users include USPTO attorneys and patent examiners, and other staff.

UCCACS is an on-demand content delivery Software as a Service (SaaS) that utilizes the CoSo Cloud, LLC – CoSo Cloud FedRAMP Managed Service Platform. The on-demand content includes Microsoft PowerPoint slides, live and recorded video, interactive slides produced Adobe using Presenter and Captivate. This system serves a variety of user groups and provides internal and external access 24 hours a day, 7 days a week. As an enterprise product, UCCACS includes the ability to interact and integrate with USPTO single sign on capabilities to provide account provisioning and authentication for internal or confidential content. That integration occurs via USPTO's ICAM IDaaS system.

Address the following elements:

(a) *Whether it is a general support system, major application, or other type of system*
UCCACS is a Major Application.

(b) *System location*
UCCACS is located in the CoSo Cloud FedRAMP managed Service Platform. All data and accompanying PII is stored in CoSo Cloud FedRAMP Managed Service Platform SaaS cloud.

(c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)*
ICAM Identity as a Service (ICAM-IDaaS) – Provides an enterprise authentication and authorization service to all applications/AIS's.

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

Enterprise Desktop Platform (EDP) – Facilitates secure access to files and applications for all USPTO employees and contractors in order to perform their day-to-day responsibilities. This includes the USPTO satellite offices.

(d) *The way the system operates to achieve the purpose(s) identified in Section 4*
UCCACS provides customers with the ability to serve on demand video to users. Authorized content administrators publish on-demand content for users to retrieve via a Uniform Resource Locator (URL). Users view the on-demand content using a browser or Adobe Connect Mobile Application via a secure Internet connection.

(e) *How information in the system is retrieved by the user*
USPTO username, login ID and email address information is retrieved by USPTO staff and contractors via web browsers on authorized USPTO computer devices and networks connected to CoSo Cloud FedRAMP Managed Service Platform Service (SaaS) cloud. Authorized USPTO staff and contractors via web browsers on authorized USPTO computer devices and networks retrieve USPTO internal video. Users via a web browser or Adobe Connect mobile application retrieve public video content.

(f) *How information is transmitted to and from the system*
Information is transmitted to and from the system via a secure Internet connection to the CoSo Cloud FedRAMP Managed Service Platform SaaS Cloud.

(g) *Any information sharing*
Authorized USPTO staff and contractors have access to the data stored on the UCCACS system. DOC OHR operation’s unit request’s that PTO post the attendance list for all mandatory USPTO/Trademark training and upload into the Learning Center to make sure the PTO OHR can send all trainee information to the Department of Commerce for compliance purposes. DOC has the ability to get these reports directly through the Learning Center.

(h) *The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information*
The citation of the legal authority to collect PII and/or BII is 5 U.S.C. 301, 35 U.S.C. 2, and E.O. 12862.

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

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☐ This is a new information system.

☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

☐ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☐	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☐	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☐	j. Home Address	☐	q. Military Service	☐

d. Gender	□	k. Telephone Number	□	r. Criminal Record	□
e. Age	□	l. Email Address	□	s. Marital Status	□
f. Race/Ethnicity	□	m. Education	□	t. Mother's Maiden Name	□
g. Citizenship	□	n. Religion	□		
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	□	e. Work Email Address	☒	i. Business Associates	□
b. Job Title	□	f. Salary	□	j. Proprietary or Business Information	□
c. Work Address	□	g. Work History	□	k. Procurement/contracting records	□
d. Work Telephone Number	□	h. Employment Performance Ratings or other Performance Information	□		
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	□	f. Scars, Marks, Tattoos	□	k. Signatures	□
b. Palm Prints	□	g. Hair Color	□	l. Vascular Scans	□
c. Voice/Audio Recording	☒	h. Eye Color	□	m. DNA Sample or Profile	□
d. Video Recording	☒	i. Height	□	n. Retina/Iris Scans	□
e. Photographs	☒	j. Weight	□	o. Dental Profile	□
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	□
b. IP Address	□	f. Queries Run	□	f. Contents of Files	□
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	□	Hard Copy: Mail/Fax	□	Online	□
Telephone	□	Email	□		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	□	Other Federal Agencies	□
State, Local, Tribal	□	Foreign	□		
Other (specify):					

Non-government Sources					
Public Organizations	□	Private Sector	□	Commercial Data Brokers	□
Third Party Website or Application			□		
Other (specify):					

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

PII in UCCACS is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Low Impact Software as a Service (LI-SaaS) Authorization. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data. Mandatory IT Awareness and role-based training is required for staff who have access to the system and addresses how to handle, retain, and dispose of data.

2.4 Is the information covered by the Paperwork Reduction Act?

□	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
☒	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	□	Biometrics	□
Caller-ID	□	Personal Identity Verification (PIV) Cards	□
Other (specify):			

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☒	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify): 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).

UCCACS is a web communication solution that enables USPTO to provide online computer-based training to internal audiences. UCCACS will be used internally by government employees and contractors and other government agencies to promote information sharing initiatives and to improve employee or customer satisfaction. Federal employees: Name, login ID, and email address etc. are collected and maintained in audit logs. It is used to capture system access. The total number of users helps to improve federal services online and as employees enjoy the convenience of the service.

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.)

Inadvertent private information exposure to foreign entities or adversarial entities as well as insider threats are risks. UCCACS implements security management controls to prevent the inappropriate disclosure of sensitive information. Automated mechanisms are in place to ensure the security of all data collected. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), the confidentiality of data in transit (Encryption), and that the data is available for authorized users only (Access Control). Management controls are utilized to prevent the inappropriate disclosure of sensitive information.

In addition, the Perimeter Network (NSI) and Security and Compliance Services (SCS) systems provide additional automated transmission and monitoring mechanisms to ensure that PII is protected and not breached by any outside entities or insider threat. USPTO has policies, procedures, and training to ensure that employees are aware of their responsibility of protecting information and the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of private information. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. In the event of disposal, UCCACS uses degaussing to permanently remove data according to government mandate and security policy.

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 The information transmitted between the systems is protected within USPTO's secure perimeter through the NSI and the SCS systems. All data transmissions are encrypted and requires credential verification. USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.
□	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: See Appendix A: USPTO Warning Banner
☐	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: USPTO employees and contractors do not have the ability to decline to provide PII since the authentication process automatically passes the user's name and USPTO email address to UCCACS via ICAM. Published on demand video content may display personal distinguishing features/biometrics (DFB).

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: USPTO employees and contractors require access to applications and the network to conduct their work. The users are required to provide their information and consent

		to its use during onboarding when they accept their USPTO PTONet credentials.

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: USPTO employees and contractors are not able to update their PII/BII within UCCACS.

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 information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 9/15/2023 ☐ 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).*

The information system provides protection of resources in accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4; the UCCACS System Security & Privacy Plan (SSPP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. The SSPP is reviewed on an annual basis. In addition, annual assessments and Continuous Monitoring reviews are conducted on RBAC. The USPTO Cybersecurity Division conducts these assessments and reviews based on NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53A Revision 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The results of these assessments and reviews are documented in the UCCACS Security Assessment Package as part of the system's Security Authorization process.

UCCACS implements security and management controls to prevent the inappropriate disclosure of information. Automated mechanism is in place to ensure the security of all data collected. Security controls are employed to ensure information is resistant to tampering (Physical and Access Controls), the confidentiality of data in transit (Encryption), and that data is available for authorized users only (Access Control). Management controls are utilized to prevent the inappropriate disclosure of information.

UCCACS is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Li-SaaS Authorization. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access and changes as part of verifying the integrity of data.

USPTO uses the Life Cycle review process to ensure that management controls are in place for UCCACS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the SSPP. The SSPP specifically addresses 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 checks on all personnel, including contractor staff. Additionally, USPTO develops privacy and PII-related policies and procedures to ensure safe handling, storing, and processing of data.

UCCACS is secured by various USPTO infrastructure components, including the NSI and SCS systems and other OCIO established technical controls to include SAML 2.0 authentication to UCCACS. Web communications leverage modern encryption technology such as TLS 1.2 over HTTPS.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-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.)*

☒	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
☐	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: UCCACS collects, maintains, or disseminates PII about DOC employees and contractors. The types of information collected, maintained, used or disseminated by the system may include Name, user id, and work email etc. which are personal identifiers. When combined, this data set can be used to identify a particular individual.
☒	Quantity of PII	Provide explanation: The number of PII user reports could be in the thousands.
☒	Data Field Sensitivity	Provide explanation: Data fields include name, login id, and email address, etc. for USPTO employees and contractors, which alone or in combination have little relevance outside the context.
☒	Context of Use	Provide explanation: Name, Login ID and email address etc. are collected and maintained in audit logs and that information is used to capture system usage. The total number of users helps to improve federal services online and as a way to measure employee satisfaction with the service for the legal work done within the Patent and Trademark offices.
☒	Obligation to Protect Confidentiality	Provide explanation: USPTO Privacy Policy requires the PII information collected within the system to be protected accordance to 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: Authorized USPTO staff and contractors have access to the data stored on the UCCACS System. UCCACS does not disseminate PII information to any other systems. PII in UCCACS is secured using appropriate administrative, physical and technical safeguards in accordance with the FedRAMP Li-SaaS Authorization.
☐	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.)

In addition to foreign and adversarial entities, insider threats, and computer failure, activity which may raise privacy concerns include the collection, maintenance, and dissemination of PII such as name, email, and voice recordings, as well as ID and date/time access. USPTO mitigates such threats through mandatory training for system users regarding appropriate handling of information and automatic purging of information in accordance with the retention schedule.

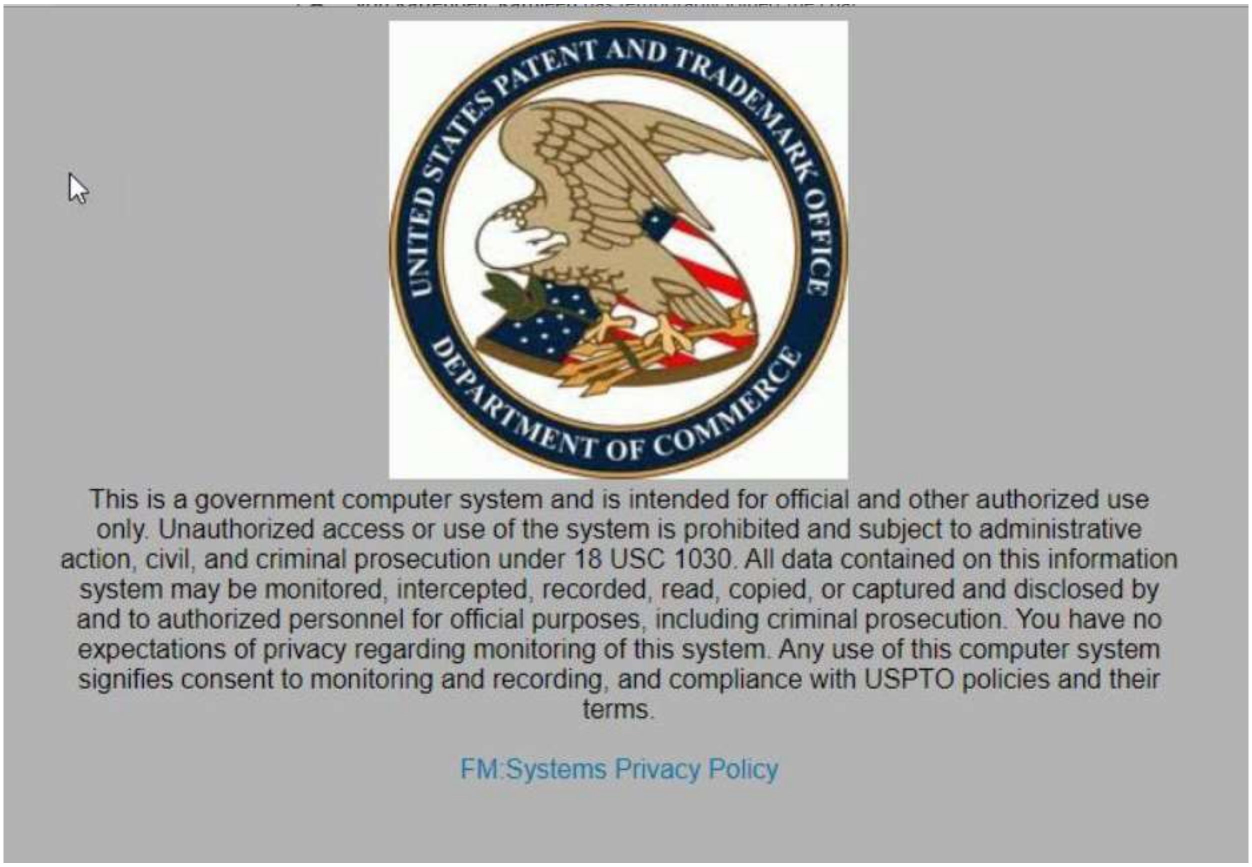
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

☐	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.

Appendix A: USPTO Warning Banner



This is a government computer system and is intended for official and other authorized use only. Unauthorized access or use of the system is prohibited and subject to administrative action, civil, and criminal prosecution under 18 USC 1030. All data contained on this information system may be monitored, intercepted, recorded, read, copied, or captured and disclosed by and to authorized personnel for official purposes, including criminal prosecution. You have no expectations of privacy regarding monitoring of this system. Any use of this computer system signifies consent to monitoring and recording, and compliance with USPTO policies and their terms.

FM:Systems Privacy Policy