Template Version Number: 01-2021

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

Privacy Impact Assessment for the Enterprise Performance Management (EPM)

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

3/31/2022

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO Enterprise Performance Management (EPM)

Unique Project Identifier: EBPL-PBG-01-00

<u>Introduction</u>: System Description

Provide a brief description of the information system.

Enterprise Performance Management (EPM) is a central planning and budgeting application supporting various organizations across the USPTO. EPM is replacing some of the technology (Oracle Hyperion Planning and Essbase) in the Enterprise Budget Tool (EBT), which is the on-premise equivalent of EPM. The software behind EPM is Oracle EPM Cloud Service to provide automation throughout the USPTO's budgeting lifecycle.

The main purpose of EPM is to allow the Office of Planning and Budget (OPB) and business units across the USPTO to project employee compensation and benefits within the current fiscal year as well as the following six fiscal years. End of year projections are calculated for each organization across the USPTO and can be compared to budgeting amounts to support analysis of results to identify causes for variances. It is also used by OPB and business units to formulate and execute their budgets.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
EPM is a FedRAMP certified Software as a Service (SaaS).

(b) System location
EPM is located within a cloud-based platform hosted by Oracle and is FedRAMP certified.

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

- **Planning and Budgeting Products (PBP)** is a master system composed of three subsystems: 1) Activity Based Information System (ABIS), 2) Analytics and Financial Forecasting (AFF), and 3) Enterprise Budgeting Tool (EBT).
- **ICAM Identity as a Service (ICAM-IdaaS)** provides enterprise authentication and authorization and National Institute of Standards and Technology (NIST) compliance.

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

EPM is a SaaS located in the cloud. Authorized users access EPM via standard internet communications protocol, TCP/IP. Oracle Data Integrator is an Extract, load and transform tool produced by Oracle that offers a graphical environment to build, manage and maintain data integration processes in business intelligence systems. EPM allows OPB and business units across the USPTO to project employee compensation and benefits within the current fiscal year as well as the following six fiscal years. End of year projections are calculated for each organization across the USPTO and can be compared to budgeting amounts to support analysis of results to identify causes for variances. It is also used by OPB and business units to formulate and execute their budgets.

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

Authorized users enter orders directly, receive orders, and make inquiries via an Internet browser.

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

USPTO follows strict guidelines regarding handling and transmitting PII/BII. Data transmitted to and from EPM is protected by secure methodologies such as Hypertext Transfer Protocol Secure (HTTPS), used for secure communication over a computer network and Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security 1.2 (TLS 1.2). Security Assertion Markup Language 2.0 (SAML 2.0) is used for exchanging authentication and authorization identities between security domains. All data stored at rest is also encrypted.

(g) Any information sharing

Information about USPTO employees and government contractors are shared within the bureau on a case-by-case basis.

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

5 U.S.C. 301, 35 U.S.C. §42(c)(3), 35 U.S.C. 3512, Budget and Accounting Act of 1921, and Fair Labor Standards Act.

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

The FIPS 199 security impact category for the system is Low.

<u>Section 1</u>: 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.

EPM 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 screen. 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.
☒	No, the information is not covered by the Paperwork Reduction Act.

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

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

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

Section 3: System Supported Activities

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

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

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	□	For administering human resources programs	□
For administrative matters	☒	To promote information sharing initiatives	☒
For litigation	□	For criminal law enforcement activities	□
For civil enforcement activities	□	For intelligence activities	□
To improve Federal services online	□	For employee or customer satisfaction	□
For web measurement and customization technologies (single-session)	□	For web measurement and customization technologies (multi-session)	□
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

EPM collects information about USPTO employees and contractors for administrative matters such as planning, and budgeting. EPM promotes information sharing initiatives by allowing various business units across USPTO to utilize the data within the system to project employee compensation and benefits within the current fiscal year as well as the following six fiscal years. End of year projections are calculated for each organization across the USPTO and can be compared to budgeting amounts to support analysis of results to identify causes for variances. EPM is also used by Office of Planning and Budgeting (OPB) and business units to formulate and execute their budgets.

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 EPM stored within the system could be exposed. In an effort to avoid a breach, EPM has put certain security controls in place to ensure that 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 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.

<u>Section 6</u>: 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: Interconnections with PII include; • PBP • ICAM-IDaaS EPM has put NIST security controls 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. 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
□	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: Individuals do not have the opportunity to decline to provide PII/BII because EPM receives PII indirectly from other application systems (front-end systems). These front-end systems provide the functionality for the data that is being collected. EPM has no authorization to decline any type of information since it is owned by the primary application.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

□	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals do not have the opportunity to consent to particular uses of their PII/BII because EPM receives PII indirectly from other application systems (front-end systems). These front-end systems provide the

		functionality for the data that is being collected.

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: USPTO employees and contractors can review/ update their PII information in the Human Resources source systems.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit logs.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): __1/31/2022_______________ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☐	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

PII within EPM is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include the Life Cycle 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 EPM 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 authorize personnel. EPM 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/DEPT-1: Attendance, Leave, and Payroll Records of Employees and Certain Other Persons COMMERCE/DEPT-18: Employees Personnel Files Not Covered By Notices of Other Agencies
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

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

	GRS 1.3, item 040 and 041, Budget Preparation Background Records GRS 1.3, item 050, Budget Administration Records GRS 5.2, item 020, Intermediary 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: Name, telephone number, user ID, and other data fields collected by EPM together identify an individual.
☒	Quantity of PII	Provide explanation: The quantity of PII corresponds to the number of USPTO employees, roughly 13,000.
☒	Data Field Sensitivity	Provide explanation: data includes personal and work-related elements used for salary and benefit projections and can cause the data fields to become more sensitive.

☒	Context of Use	Provide explanation: PII is used for administrative purposes such as planning and budgeting.
☒	Obligation to Protect Confidentiality	Provide explanation: 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); Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: PII is hosted by a FEDRAMMP authorized cloud provider. The information captured, stored, and, transmitted by the EPM system is accessible by internal USPTO employees and contractors with access permissions.
	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 is such as user ID, name, work email address, and work phone number pose 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 zones 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 an 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.

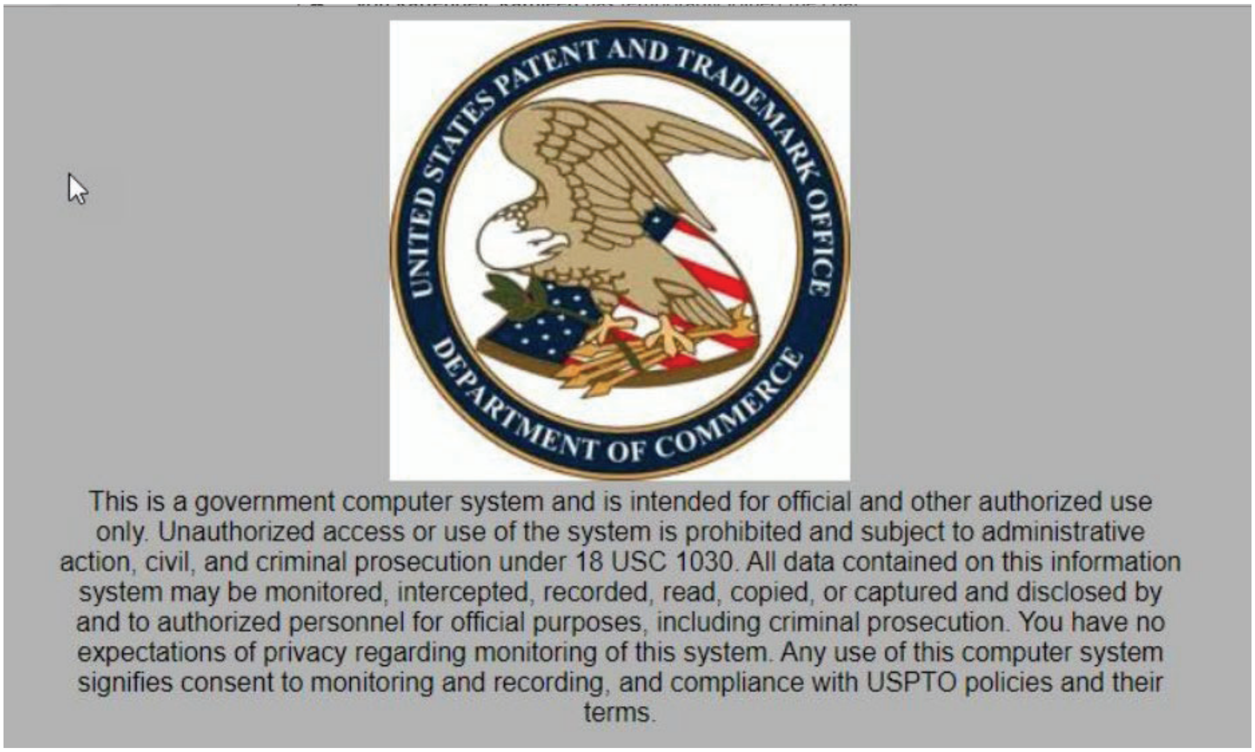
12.2 Indicate whether the conduct of this PIA results in any required business process changes.

☐	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.

Appendix A: USPTO Notice



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.