Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Enterprise Performance Management (EPM)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Enterprise Performance Management (EPM)

Unique Project Identifier: EBPL-PBG-01-00

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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 purpose that the system is designed to serve

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) The way the system operates to achieve the purpose

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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

EPM collects information about USPTO employees related to employee compensation and benefits. Information in the system may include: employee ID, name, occupation, job title, work address, work telephone number, work email address, and salary.

g) Identify individuals who have access to information on the system

Individuals with access to the information on the system include authorized USPTO employees and contractors.

h) How information in the system is retrieved by the user

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

i) 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☒ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

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

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☒ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☐ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

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

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees
☒ Contractors working on behalf of DOC
☐ Other Federal Government personnel
☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☐ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

☒ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☐ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☒ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the **Enterprise Performance Management (EPM)** and as a consequence of this applicability, I will perform and document a PIA for this IT system.

☐ I certify the criteria implied by the questions above **do not apply** to the **Enterprise Performance Management (EPM)** and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Christopher D. Tegarden Office: Planning and Budget Products Division (C/PBPD) Phone: (571) 272-8423 Email: Christopher.tegarden1@uspto.gov Signature: Users, Tegarden, Christopher — Digitally signed by Users, Tegarden, Christopher Date: 2022.02.16 09:50:37 -05'00' Date signed: _____	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: Users, Watson, Don — Digitally signed by Users, Watson, Don Date: 2022.02.16 16:24:07 -05'00' Date signed: _____
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 270-1557 Email: Ezequiel.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel — Digitally signed by Users, Berdichevsky, Ezequiel Date: 2022.02.16 09:29:39 -05'00' Date signed: _____	**Bureau Chief Privacy Officer and Co-Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry — Digitally signed by Users, Holcombe, Henry Date: 2022.02.18 12:29:32 -05'00' Date signed: _____
Co-Authorizing Official Name: Dennis Hoffman Office: Office of the Chief Financial Officer (C/CFO) Phone: (571) 272-7262 Email: Jay.Hoffman@uspto.gov Signature: Users, Hoffman, Dennis (Jay) — Digitally signed by Users, Hoffman, Dennis (Jay) Date: 2022.03.08 11:50:07 -05'00' Date signed: _____	

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