

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



**Privacy Threshold Analysis
for the
Adobe Experience Manager- Managed Services (AEM-MS)**

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Adobe Experience Manager- Managed Services (AEM-MS)

Unique Project Identifier: EIPL-DS-10-00

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).

Adobe Experience Manager-Managed Services (AEM-MS) is a general support enterprise service for signatures. The service provides a verifiable digital Trademark certificate to the user that they can access by clicking on the certificate details. The system is deployed as a Software as a Service (SaaS) platform with Adobe Corporation managing and maintaining infrastructure and software. The information within the system is encrypted to address security and privacy concerns. USPTO is responsible for Hardware Security Manager (HSM), which is hosted on premises and managed by the USPTO Public Key Infrastructure (PKI) team.

Address the following elements:

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

AEM-MS is a general support system (GSS).

b) *System location*

AEM-MS is a SaaS system hosted in the Amazon Web Services (AWS) cloud, which is Federal Risk and Authorization Management (FedRAMP) Certified. There is a Hardware Security Module deployed on-premise at the USPTO Alexandria, Virginia Data center.

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

AEM-MS is interconnected to:

Patent End to End (PE2E) - provides examination tools for Central examination unit to track and manage the cases in this group and view documents in text format.

Patent Capture and Application Processing System – Capture and Initial Processing (PCAPS-IP) – provides support to the USPTO for the purposes of capturing patent applications and related metadata in electronic form; processing applications electronically; reporting patent application processing and prosecution status; and retrieving and displaying patent applications.

Patent Business and Content Management Services (PBCMS) EventHub (EventHub) – provides file transformation functionality for the USPTO enterprise.

Trademark External (TM External) – comprised of different search components: TM External Filing (EFile), Trademark Status & Document Retrieval Services (TSDR), Trademark Last Updated Service (TM-LUS), TrademarkVision (TMVision), TM Pre-Examinations Automated Batch Search (TM-PEA-ABS), and Trademark Electronic Official Gazette (TM-EOG).

d) The purpose that the system is designed to serve

The system provides signature services for USPTO applications.

e) The way the system operates to achieve the purpose

AEM-MS is a general support service for signatures. The service provides a verifiable digital Trademark certificate to the user that they can access by clicking on the certificate details. The system is deployed as a SaaS platform with Adobe Corporation managing and maintaining infrastructure and software. The information within the system is encrypted to address security and privacy concerns. USPTO is responsible for Hardware Security Manager (HSM), which is hosted on premises and managed by the USPTO Public Key Infrastructure (PKI) team.

The integrated applications submit a document requiring signature. The system accepts the document (through Hyper Text Transfer Protocol Secure (HTTPS) Representational State Transfer (REST) based Application Programming Interfaces (APIs)) and based on the configurations and authorization the system signs the document based on the credentials that are stored in the Hardware Security Module.

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

The system does not collect, maintain and/or disseminate any information. The documents are processed only for signature on other information obtained and/or stored from the documents. The signature logs are generated for auditing and non-repudiation purpose.

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

Only the system administrators have access to the system configurations. All other interactions are conducted between systems over Transfer Layer Security (TLS) 1.2 or higher.

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

Users do not have access to the system. Users are not able to access any information from the system. All interactions are system to system over TLS 1.2 or higher. Only the administrators have access to system configurations.

i) How information is transmitted to and from the system

All communication is between systems and/or administrative console. All communication is encrypted over TLS 1.2 higher using HTTPS protocols.

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	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
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

- ☒ The criteria implied by one or more of the questions above **apply** to the Adobe Experience Manager- Managed Services (AEM-MS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.
- ☐ The criteria implied by the questions above **do not apply** to the Adobe Experience Manager-Managed Services (AEM-MS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Jimmy Orona III Office: Enterprise Software Services Division Phone: (571) 272-0673 Email: Jimmy.Orona@uspto.gov Signature: _____ 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: _____ 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: _____ Date signed: _____	Bureau Chief Privacy Officer and Authorizing Official Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: _____ Date signed: _____
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: _____ Date signed: _____	