Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Executive Document Management System Cloud (EDMS-C)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Executive Document Management System Cloud (EDMS-C)

Unique Project Identifier: PTOC-042-00

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).

The Executive Document Management System Cloud (EDMS-C) is an application information system, used by the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office to receive and respond to a wide range of official correspondence, by electronically capturing, routing, and tracking both incoming and response documents, thereby improving workflow. EDMS-C also serves as an electronic repository of documents such as Action Decision Memoranda, Congressional Inquiries, Federal Registry Notices, Delegations of Authority, Public Advisory Committee (PAC) Nomination Process, and General Letters to the Agency. EDMS-C also records the status of all actions taken on official correspondence and creates immediate activity reporting and provides users a graphical user interface via a Web browser.

Address the following elements:

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

b) *System location*

Cloud based services platform hosted by Leidos Digital Solutions, Inc.

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

EDMS-C interconnects with:

Enterprise Desktop Platform (EDP) - The EDP is an infrastructure information system which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 7 and Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations.

Enterprise Software Services (ESS) - ESS provides Enterprise Directory Services, Role-Based Access Control System, Email as a Service, PTO Exchange Services, Symantec Endpoint Protection, Enterprise SharePoint Services, etc.

Enterprise UNIX Services (EUS) - EUS consists of assorted UNIX operating system variants (OS), each comprised of many utilities along with the master control program, the kernel.

Enterprise Windows Services (EWS) - EWS is an Infrastructure information system, and provides a hosting platform for major applications that support various USPTO missions.

Network and Security Infrastructure System (NSI) - NSI is an Infrastructure information system, and provides an aggregate of subsystems that facilitates the communications, secure access, protective services, and network infrastructure support for all United States Patent and Trademark Office (USPTO) IT applications.

Security and Compliance Services (SCS) - SCS provides a centralized command and control console with integrated enterprise log management, security information and event management, network behavior analysis, and reporting through the collection of events, network/application flow data, vulnerability data, and identity information.

Service Oriented Infrastructure (SOI) - SOI provides a feature-rich and stable platform upon which USPTO applications can be deployed.

d) *The purpose that the system is designed to serve*

The system is used by the Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office to receive and respond to a wide range of official correspondence, by electronically capturing, routing, and tracking both incoming and response documents, thereby improving workflow.

e) *The way the system operates to achieve the purpose*

The system operates by generating actions, tracking the status of actions, recording data, and improving the use of automated tools to schedule, manage and monitor follow up of information and documents among staff.

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

EDMS-C collects and maintains some PII from Public Advisory Committee applicants, inventors, federal, state, and local officials, and members of the public.

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

USPTO employees and contractors.

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

USPTO users have access to the EDMS-C system through a web interface that utilizes Single Sign on (SSO). The access level defines if they have access to the PII information. When an attachment is either created or requested, EDMS-C waits for the file to be modified on the user's workstation. If it is changed, the system asks the user if the updated version should be sent back to the server. The file is easily uploaded without further user intervention.

i) How information is transmitted to and from the system

Information is gathered from the public users and access by internal users using an interface secured by HTTP forwarded to HTTPS to which requests receive responses in the form of HTML pages that are sent back to the user for display in a Web browser.

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

☒ The criteria implied by one or more of the questions above **apply** to the Executive Document Management System Cloud (EDMS-C) 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 Executive Document Management System Cloud (EDMS-C) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Patrick Barcia Office: Office of the Secretary and Director(U/DIR) Phone: (571) 272-5163 Email: Patrick.Barcia@uspto.gov Signature: Patrick B. Barcia Digitally signed by Patrick B. Barcia Date: 2023.08.01 14:07:29 -04'00' Date signed: 8/1/2023	**Chief Information Security Officer** Name: Timothy S. Goodwin Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-0653 Email: Timothy.Goodwin@uspto.gov Signature: Users, Goodwin, Timothy Digitally signed by Users, Goodwin, Timothy Date: 2023.08.17 16:06:17 -04'00' Date signed:
Privacy Act Officer Name: Heaton John Office: Office of General Law (O/GL) Phone: 703-756-1240 Email: Ricou.Heaton@uspto.gov Signature: John Ricou Heaton Digitally signed by John Ricou Heaton Date: 2023.08.08 09:02:00 -04'00' 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: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.08.18 09:26:13 -04'00' Date signed:
Co-Authorizing Official Name: N/A Office: N/A Phone: N/A Email: N/A Signature: Date signed:	