Version Number: 01-2019

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

Privacy Threshold Analysis
for the
Landon IP Information System

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Landon IP Information System

Unique Project Identifier: [1861] PTOC-019-00

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 and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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 LIPIS is an infrastructure information system that is designed to support the USPTO international application or PCT application process. The Patent Cooperation Treaty (PCT) provides a unified procedure for filing patent applications to protect inventions in each of its Contracting States. The LIPIS facilitates PCT searches and enables Landon IP employees to submit an accompanying written opinion regarding the patentability of the invention in question.

Landon IP is under contract with the USPTO to perform work related to PCT applications. Landon IP receives PCT application data from the USPTO via SFTP, a secure file transfer system based on the SSH protocol. Utilizing this data, Landon IP conducts searches and develops opinion papers for the USPTO.

In support of this contract with the USPTO, Landon IP has implemented the LIPIS. The LIPIS is the automated information system comprised of the Landon IP network environment that supports the USPTO. The LIPIS was developed to provide a comprehensive set of security controls to adequately protect USPTO data. The LIPIS is a networked system of servers, equipment, and applications that meet the requirements for the General Support System/Infrastructure System.

a) ***Whether it is a general support system, major application, or other type of system***
   The Landon IP Information System (LIPIS) is a General Support System.
b) ***System location***
   LIPIS is located in Reston, VA.
c) ***Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)***

LIPIS interconnects with the Network and Security Infrastructure (NSI).

d) The purpose that the system is designed to serve

The purpose of LIPIS is to assist USPTO in processing Patent Applications.

e) The way the system operates to achieve the purpose

LIPIS operates by receiving patent applications from USPTO, storing the data and distributing it to LIPIS staff to conduct searches and develop opinion papers. Completed deliverables are returned from LIPIS to USPTO.

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

Bibliographic data: Inventor name, Inventor address, Citizenship, Correspondence address, Employer name and address, Telephone number(s), E-mail address, Occupation and Business associates.

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

Landon IP personnel consisting of system administrators, managers and analysts who assign, review conduct searches and develop option papers.

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

LIPIS receives the information from USPTO and stores it on a file server for review and assignment. Assigned applications are accessed by analysts who connect to LIPIS via Remote Desktop Protocol (RDP). Completed applications are stored on the file server and returned to USPTO.

i) How information is transmitted to and from the system

Data transmitted between LIPIS and USPTO uses an end-to-end secure file transfer solution.

Questionnaire:

1. 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 (version 01-2015).
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 (version 01-2017 or later). *Skip questions and complete certification.*

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 personally identifiable information (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

☐ National Institute of Standards and Technology Associates
☐ 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 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 Landon IP Information System 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 Landon IP Information System and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of System Owner (SO): Blaine Copenheaver

Signature of SO: Users, Copenheaver, Blaine Digitally signed by Users, Copenheaver, Blaine Date: 2021.02.25 09:00:13 -05'00' Date: _____

Name of Privacy Act Officer (PAO): John (Ricou) Heaton

Signature of PAO: Users, Heaton, John (Ricou) Digitally signed by Users, Heaton, John (Ricou) Date: 2021.02.24 13:59:29 -05'00' Date: _____

Name of Chief Information Security Officer (CISO): Don Watson

Signature of CISO: DON R Watson Digitally signed by DON R Watson Date: 2021.03.01 14:20:37 -05'00' Date: _____

Name of Authorizing Official (AO) & Bureau Chief Privacy Officer (BCPO): Henry J. Holcombe

Signature of AO & BCPO: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2021.03.03 12:02:36 -05'00' Date: _____

Name of Authorizing Official (AO) or Designated Representative: Andrew Faile

Signature of AO: Users, Faile, Andrew Digitally signed by Users, Faile, Andrew Date: 2021.03.05 12:54:34 -05'00' Date: _____