Template Version Number: 01-2021

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

## Privacy Impact Assessment
## for the
## Landon IP Information System (LIPIS)

☒ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

CHARLES CUTSHALL Digitally signed by CHARLES CUTSHALL
Date: 2024.12.05 18:04:18 -05'00' 12/5/2024

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

# U.S. Department of Commerce Privacy Impact Assessment
# USPTO Landon IP Information System (LIPIS)

**Unique Project Identifier: PTOC-019-00**

**Introduction: System Description**

*Provide a brief description of the information system.*

The Landon IP Information System (LIPIS) is an infrastructure information system that is designed to support the United States Patent and Trademark Office (USPTO) international application or Patent Cooperation Treaty (PCT) application process. The 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 Secure File Transfer Protocol (SFTP), a secure file transfer system based on the Secure Shell (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.

Address the following elements:

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

LIPIS is a Major Application system.

*(b) System location*

LIPIS is located a Data Center in Virginia.

*(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 system below:

**Network and Security Infrastructure (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 USPTO IT applications.

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

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.

*(e) 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.

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

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

*(g) Any information sharing*

LIPIS shares information with USPTO and International patent offices based on the PCT.

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

35 U.S.C. 1, 2, 41, 115, and 361; E.O. 9424; 5 U.S.C. 301

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

Moderate

## Section 1: 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): Registration number, Patent Application number, Agent File reference number, Deposit Account number | | | | | |
| *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): Fax number | | | | | |

| **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.

LIPIS encrypts data during transmission, performs incremental and full backups, unusual activity is logged and audited prompting review, and logical and physical access controls are leveraged to limit access to the system and its data to authorized individuals. LIPIS also uses best practice hashing techniques to ensure the integrity of the data that is stored within the system. Finally, USPTO requires annual security role-based training and annual mandatory security awareness procedure training for all employees handling LIPIS data.

2.4 Is the information covered by the Paperwork Reduction Act?

| | |
|---|---|
| ☒ | Yes, the information is covered by the Paperwork Reduction Act.<br>Provide the OMB control number and the agency number for the collection.<br>0651-0031 Patent Processing<br>0651-0032 Initial Patent Application |
| ☐ | 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): Click or tap here to enter text. | | | |

| | |
|---|---|
| ☒ | 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).

The PII and/or BII data is collected by the USPTO to facilitate the patent application and classification process. The PII/BII comes from persons applying for patents through the USPTO or where the USPTO is acting as an International Searching Authority for a foreign filed international application. This could include members of the public. Filing of an application is accompanied with a search report and a written opinion regarding the patentability of the invention which is the subject of the application.

Under the terms and conditions of the PCT, the USPTO serves as a Receiving Office, an International Searching Authority and an International Preliminary Examination Authority for international patent applications filed in accordance with the PCT. A single filing of an international application is accompanied with a search report and a written opinion regarding the patentability of the invention which is the subject of the application. Applicants are required to provide the information to the Receiving Office, in this case the USPTO, as part of the application process.

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.)

Nation states and adversarial entities are the predominant threats to the information collected and its privacy. The system has implemented security controls following NIST guidance to deter and prevent threats to privacy. Controls implemented enforce physical and logical access; auditing of system, application and security events; encryption of data at rest and in transit, hashing, Non-disclosure Agreements; and security awareness training.

NIST security controls are 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. 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.

## Section 6: 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.<br>Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: |
| ☒ | 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: Notice is provided at the time of collection by the Patent Capture and Application Processing System – Initial Processing (PCAPS-IP). |
| ☐ | 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: LIPIS does not collect the PII/BII directly from the individual. Individuals' rights to decline to provide their PII/BII would be in the source system. PCAPS-IP. |

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: LIPIS does not collect the PII/BII directly from the individual. Individuals consent to particular uses of their PII/BII would be in the source system. PCAPS-IP. |

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

| | | |
|---|---|---|
| ☐ | Yes, individuals have an opportunity to | Specify how: |

| | | |
|---|---|---|
| | review/update PII/BII pertaining to them. | |
| ☒ | No, individuals do not have an opportunity to review/update PII/BII pertaining to them. | Specify why not:<br>Individuals do not have the opportunity to update the PII/BII directly in LIPIS. During patent submission via PCAPS-IP EFSWeb and PE2E, Patent Center, applicants have opportunities to update PII/BII data prior to final submission. After a patent submission, users must contact the Electronic Business Center for PII/BII updates. All subsequent PII/BII updates occur within PCAPS-ES and PE2E systems. |

## 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.<br>Explanation: System and application auditable events are leveraged to monitor, track and record access to PII/BII. |
| ☒ | The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements.<br>Provide date of most recent Assessment and Authorization (A&A): 12/26/2023<br>☐ 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 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). |
| ☒ | 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).*

| |
|---|
| Controls implemented enforce physical and logical access; auditing of system, application and security events; encryption during transmission; and security awareness training. PII/BII within the system 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 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. The system 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).<br>Provide the SORN name, number, and link. *(list all that apply)*:<br><br>PAT-TM-7 Patent Application Files<br>PAT-TM-10 Deposit Accounts and Electronic Funds Transfer Profiles |
| ☐ | 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.)*

General Records Schedules (GRS) | National Archives

| | |
|---|---|
| ☒ | There is an approved record control schedule.<br>Provide the name of the record control schedule:<br>Patent Case Files, Granted (N1-241-10-1:2)<br>Abandoned Patent Applications, Not Referenced in Granted Case File (N1-241-10-1:3)<br>Patent Examination Working Files (N1-241-10-1:4.2) |
| ☐ | No, there is not an approved record control schedule.<br>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:<br>Inventor name, Inventor address, Citizenship, Correspondence address, Employer name and address, Telephone number[s], and E-mail address can easily identify an individual. |
| ☒ | Quantity of PII | Provide explanation:<br>LIPIS continuously receives and returns thousands of patent applications containing PII information. |
| ☒ | Data Field Sensitivity | Provide explanation:<br>The combination of Inventor name, Inventor address, Citizenship, |

| | | |
|---|---|---|
| | | Correspondence address, Employer name and address, Telephone number[s], and E-mail addresses of thousands of patent applications can make the data fields more sensitive. |
| ☒ | Context of Use | Provide explanation:<br>Information is for identifying and tracking patent applicants & applications. |
| ☒ | Obligation to Protect Confidentiality | Provide explanation:<br>USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974 and USPTO Privacy Policy requires the PII information collected within the system to be protected in accordance with NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information. |
| ☒ | Access to and Location of PII | Provide explanation:<br>Because the information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during transmission.<br><br>There is no PII stored within the LIPIS system. Staff PII data is stored within Clarivate Human Resources. |
| ☐ | 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.)

| |
|---|
| Nation states and adversarial entities are the predominant threats to the information collected and its privacy. Security controls following NIST guidance were implemented to deter and prevent threats to privacy. USPTO has identified and evaluated potential threats to PII such as loss of confidentiality and integrity of information. Based upon USPTO's threat assessment policies, procedures, and training has been implemented to ensure that employees are aware of their responsibility to protect PII and to be aware of insider threats. Our employees are aware of the negative impact to the agency if there is a loss, misuse, or unauthorized access to or modification of PII. |

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.<br>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.<br>Explanation: |
| ☒ | No, the conduct of this PIA does not result in any required technology changes. |