Template Version Number: 01-2021

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

Privacy Impact Assessment
for the
OpenWater LI-SaaS (OpenWater LI-SaaS)

Reviewed by: Henry J. Holcombe, Bureau Chief Privacy Officer

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

Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry
Date: 2023.04.07 14:22:34 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
USPTO OpenWater LI-SaaS (OpenWater LI-SaaS)

Unique Project Identifier: EBPL-CCE-01-00

Introduction: System Description

Provide a brief description of the information system.

OpenWater LI-SaaS (OpenWater LI-SaaS) is a general-purpose application and review system. USPTO uses OpenWater LI-SaaS to collect and review nominations of individuals, teams, and organizations for various award programs. Low impact, non-mission critical information can be collected by OpenWater LI-SaaS and centralized for reviewers to provide scores and feedback.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system
OpenWater is Li-SaaS application.

(b) System location
OpenWater is Li-SaaS application hosted in Microsoft Azure Commercial Cloud.

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
ICAM Identity as a Service (ICAM-IdaaS) provides authentication and authorization services to all enterprise USPTO applications and information systems.

PTONet System (PTONet) provides the common network which connects all USPTO applications and network access for employees, contractors, Public Search Room visitors to applications and systems in IT-East and IT-West data centers.

(d) The way the system operates to achieve the purpose(s) identified in Section 4
OpenWater LI-SaaS is a web-based awards management software to support the USPTO administration various award programs. Members of the public submit nominations and then a committee of judges evaluates and scores the nominations within the system. Nominators and judges have their own unique login information to access the system. USPTO employees and

contractors have administrative access and can change the nomination or judging process as needed.

(e) How information in the system is retrieved by the user
Nominators, judges, and USPTO employees and contractors will access OpenWater LI-SaaS using a web interface.

(f) How information is transmitted to and from the system
Information is transmitted to and from OpenWater LI-SaaS over the internet. Data flow to and from the system via Hypertext Transfer Protocol Secure (HTTPS) and is secured using Transport Layer Security (TLS) 1.2 protocol.

(g) Any information sharing
Information in the system will be shared within the bureau and other federal agencies on a case-by-case basis

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
15 U.S.C. § 3711 and Stevenson Wydler Technology Innovation Act of 1980.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system
OpenWater LI-SaaS has a FIPS 199 security impact category of Low.

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):					
*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):

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.

Open Water LI-SaaS is secured using appropriate administrative, physical, and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screen. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

2.4 Is the information covered by the Paperwork Reduction Act?

☒	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. OMB Control No. 0651-0060
☐	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): For administration of nominations used to recognize high achievers in the industry.			

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).

OpenWater LI-SaaS collects and maintains PII from USPTO employees, contractors, other federal government personnel, and members of the public for administrative matters. OpenWater LI-SaaS disseminates PII to USPTO employees, contractors, other federal government personnel for administrative matters. USPTO uses OpenWater LI-SaaS to collect and review nominations of individuals, teams, and organizations for the NMTI for the purposes of recognizing individuals with extraordinary capabilities. USPTO administers this award on behalf of the White House and DOC. Low impact, non-mission critical information can be collected by OpenWater LI-SaaS and centralized for reviewers to provide scores and feedback.

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.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data OpenWater LI-SaaS stores within the system could be exposed. To avoid a breach, OpenWater LI-SaaS has put certain security controls in place to ensure that information is handled, retained, and disposed of appropriately. 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. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

OpenWater LI-SaaS has put certain security controls 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. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO- POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36).
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.

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. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: Open Water LI-SaaS connects with ICAM-IdaaS which provides authentication and authorization services to all enterprise USPTO applications and AIS's. Open Water LI-SaaS has put certain security controls 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. The following are current USPTO policies; Information Security Foreign Travel Policy (OCIO-POL-6), IT Privacy Policy (OCIO-POL-18), IT Security Education Awareness Training Policy (OCIO-POL-19), Personally Identifiable Data Removal Policy (OCIO-POL-23), USPTO Rules of the Road (OCIO-POL- 36). 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.
☐	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: Appendix A
☐	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: Yes, individuals can decline to provide PII by not applying. The application process is voluntary.
☐	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: Yes, individuals can consent to uses of their PII. At the end of the application there is a consent section where the nominator can enter which information is not for public disclosure.
☐	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Yes, individuals have an opportunity to review/update PII pertaining to them. All information can be edited during the nomination window.
☐	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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. Explanation: Audit logs.
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 12/30/2022 ☐ 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 4 Appendix J 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): USPTO employees and contractors signed a confidentiality agreement or non-disclosure agreement and are subject to a Code of Conduct that includes the requirement for confidentiality.

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).*

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4, the Open Water LI-SaaS System Security Plan (SSP) addresses the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment. PII within Open Water LI-SaaS 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 data to a small subset of Open Water LI-SaaS 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. Open Water LI-SaaS maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity.

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). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/PAT-TM-21 National Medal of Technology and Innovation Nominations
☐	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.)*

☒	There is an approved record control schedule. Provide the name of the record control schedule: N1-241-09-1:a2.4, Unsuccessful Nomination Files and GRS 5.1, item 020, Non-Recordkeeping Copies of Electronic Records NOTE: The system may also contain some records covered under N1-241-09-1:a2.3, NMTI Program Subject Files
☐	No, there is not an approved record control schedule. 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: PII collected includes general personal and work-related data such as name, email, and work address etc. together could identify a particular individual.
☒	Quantity of PII	Provide explanation: The quantity of PII will be determined by the number of nominations submitted for review.
☒	Data Field Sensitivity	Provide explanation: Work-related data such as proprietary or business information could make the data field more sensitive.
☒	Context of Use	Provide explanation: PII submitted is about individuals, teams, and organizations who have been nominated for the NMTI award. The system will centralize the collection of information for reviewers to provide scores and feedback.
☒	Obligation to Protect Confidentiality	Provide explanation: NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M); Privacy Act of 1974.
☒	Access to and Location of PII	Provide explanation: PII is in a FIPS 199 Low system. The information captured, stored, and, transmitted by the OpenWater LI-SaaS system is accessible by internal USPTO employees and contractors and judges with access permissions
☐	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.)

The PII in this system is such as user ID, name, email address and phone number etc. are publicly available information but the proprietary information included may pose some privacy risk. System users undergo annual mandatory training regarding appropriate handling of information. Judges receive Ethics training prior to review of nominations. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are in secure zones and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

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

Appendix A

Your Nomination has been received, the information below is read only

General Information → Summary of Nominee's Contribution/Achievement → Nominee Biographical Information → Nominator Information → Letters of Recommendation → Compliance with Program Terms

Compliance with Program Terms

I, the nominator, of my nominee for a National Medal of Technology and Innovation award, by my submission of this nomination do hereby consent to public disclosure of the information contained in this package for the purpose of use or distribution by the Department of Commerce to develop descriptive material, such as magazine articles, Web sites or other means, to increase public awareness of National Medal of Technology and Innovation Laureates and their accomplishments. I do **NOT** consent to public disclosure of any information deemed personal, as noted below:

The Department of Commerce requests that recipients of the National Medal of Technology and Innovation work with its agencies and the National Science and Technology Medals Foundation to share additional information about "lessons learned" regarding U.S. commercial process and competitiveness.

The public reporting burden for the collection of this information is estimated to average 40 hours per response, including the time for reviewing instructions, collecting information, and completing the form. All responses to this request for information are voluntary for purposes of the Paperwork Reduction Act. Please mark clearly any portion of the information submitted that you consider to be proprietary and it will be afforded confidentiality to the extent allowed under the Freedom of Information Act. Notwithstanding any other provision of law, no person is required to respond to, nor shall a person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act unless that collection of information displays a current valid OMB control number. Comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, can be sent to the Chief Administrative Officer, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 (NMTI@uspto.gov).

Privacy Act Statement

The United States Patent and Trademark Office (USPTO) collects this information under authority of 15 USC 3711. The information in this system of records is used to manage records such as name, postal address, telephone number, e-mail address, citizenship, employment history, and other information pertaining to an individual's activities, statements containing various kind of information with respect to the contributions of the individual(s) and/or group(s). The information you provide is protected from disclosure to third parties in accordance with the Privacy Act.

However, routine uses of this information may include disclosure to the following: to law enforcement and investigation in the event that the system of records indicates a violation or potential violation of law; to a Federal, state, local, or international agency, in response to its request; to an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law; to non-federal personnel under contract to the agency; to a court for adjudication and litigation; to the Department of Justice for Freedom of Information Act (FOIA) assistance; to members of congress working on behalf of an individual; to the Office of Personnel Management (OPM) for personnel research purposes; to National Archives and Records Administration for inspection of records. Failure to provide any part of the requested information may result in an inability to process nominations. The applicable Privacy Act System of Records Notice for this information is COMMERCE/PAT-TM-21 National Medal of Technology and Innovation Nominations: Federal Register / Vol. 73, No. 18 / Monday, January 28, 2008 / Notices 4851 available at https://www.uspto.gov/sites/default/files/sorn/uspto-pasorn-21.pdf.

Administered by
The United States Patent and Trademark Office
U.S. Department of Commerce

OMB Approval No. 0651-0060

Points of Contact and Signatures

System Owner
Name: Linda Hosler
Office: Office of the Chief Communications Officer (C/CCO)
Phone: (571) 272-8514
Email: Linda.Hosler@uspto.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Hosler, Linda Digitally signed by Users, Hosler, Linda Date: 2023.04.05 08:01:48 -04'00'

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

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2023.04.07 10:25:00 -04'00'

Date signed: _____

Privacy Act Officer
Name: Kyu Lee
Office: Office of General Law (O/GL)
Phone: (571) 272-6421
Email: Kyu.Lee@uspto.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: Users, Lee, Kyu S. Digitally signed by Users, Lee, Kyu S. Date: 2023.04.04 17:31:52 -04'00'

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

I certify that the PII/BII processed in this IT system is necessary, this PIA ensures compliance with DOC policy to protect privacy, and the Bureau/OU Privacy Act Officer concurs with the SORNs and authorities cited.

Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.04.07 14:23:00 -04'00'

Date signed: _____

Co-Authorizing Official
Name: Russell Lopez
Office: Office of the Chief Communications Officer (C/CCO)
Phone: (571) 272-8400
Email: Russell.Lopez@uspto.gov

I certify that this PIA accurately reflects the representations made to me herein by the System Owner, the Chief Information Security Officer, and the Chief Privacy Officer regarding security controls in place to protect PII/BII in this PIA.

Signature: Users, Lopez, Russell Digitally signed by Users, Lopez, Russell Date: 2023.04.11 10:59:28 -04'00'

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 PIA.