

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



**Privacy Impact Assessment
for the
Corporate Administrative Office System (CAOS)**

Reviewed by: John B. Owens II, 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

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

Date

U.S. Department of Commerce Privacy Impact Assessment USPTO Corporate Administrative Office System (CAOS)

Unique Project Identifier: PTOC-005-000

Introduction: System Description

(a) A general description of the information in the system:

The Corporate Administrative Office System (CAOS) is an Application information system. The purpose of the CAOS is to support the Human Resources business functions within the United States Patent and Trademark Office (USPTO). The CAOS is composed of three (3) Automated Information Systems (AISs) that provide the following capabilities:

- Allows USPTO employees' Time and Attendance information to be entered, verified, electronically certified and collected for transmission via PTONet and OHRNet to the Department of Agriculture's National Finance Center's (NFC) personnel/payroll system.
- A broad range of data processing and management capabilities including specialized features, capabilities to provide the Office of Security & Safety the ability to track and manage data.
- Rapid dissemination of emergency notifications to targeted USPTO personnel working on campus and/or remotely.

The CAOS consists of the following three (3) subsystems:

WebTA allows the United States Patent and Trademark Office (USPTO) time and attendance information to be entered, verified, and electronically certified. The information is then collected for transmission to the NFC's personnel/payroll system in accordance with existing policies and procedures.

WebTA provides the following functionality:

- Provide a Web based intranet interface for all USPTO employees
- Allow the automated entry, saving and storing of T&A data on a 24-hour per day/7 days per week availability (except during maintenance)
- Generate and send e-mail messages and task information using USPTO email addresses
- Gather information for the PTO Leave Donor Program

ENS is a network-based emergency notification system which provides rapid dissemination of emergency messages to USPTO personnel. It enables the Office of Security to provide emergency information and instructions agency-wide or to a targeted building and, when beneficial, to receive feedback through responses to the message. Through an audible alert and visual desktop popup text message. It is a rapid and effective means of notifying the entire USPTO community (10,000+ employee workstations) in less than 5 minutes so they may react

quickly in an emergency. This includes those working from a remote location (teleworking) as well as those on campus.

- The ENS uses an alert management COTS software to provide a scalable central solution for Network Alerts emergency notification systems.
- It is widely used by several federal agencies including The Department of Defense, US Coast Guard, Department of Energy and Department of Veteran's Affairs.
- The USPTO Office of Security can issue pre-scripted or ad hoc messages from any web browser enabled computer with access to the USPTO network (as well as via VPN).
- Agency ENS administrators can create, manage, and send alerts to any computer using a standard web browser. Alerts can be designated to a targeted recipient by specific department or location.
- The Office of Security can track alerts that are maintained in an audit trail that shows exactly which personnel received and acknowledged each alert.

COOP-WB is a replacement of the existing Continuity of Operations Plan Work Book (COOP-WB) with a more efficient electronic, web-based solution, accessible to other COOP-WB representatives. In addition to being a simpler and less time-consuming method for Business Unit COOP-WB managers and assistants to complete and maintain their portion of the overall USPTO COOP-WB/Plan, the data contained in the work is accessible/retrievable for inclusion in reports that improve the agency's ability to reconstitute following an emergency or disaster.

COOP-WB uses the COTS software from Sustainable Planner, which greatly reduce the amount of time agency continuity personnel spends completing the BCCP and workbooks and provides reports that are vastly superior to the manual outputs possible from existing documents. USPTO should be able to rapidly generate a list of downstream impacts to/from any pinpointed failure, from any automated information system to a particular building. This should provide critical data/information to the agency during a continuity event and could decrease the amount of time to return the agency to full operational status.

(b) A description of a typical transaction conducted on the system:

WebTA: Allows USPTO employees to record, track, validate and certify their time and attendance. Complete payroll and personal transactions including Statements of Earnings and Leave, quick service payments, final salary payments for indebted employees, payments to the estate of a deceased employee, view and print a USPTO employee's W-2, and Wage and Tax Statement data.

COOP-WB: Allows authorized emergency management personnel and COOP Business Unit managers and assistants to input Continuity of Operation information such as business impacts, line of succession, critical IT applications and processes, staff/employee personal information, and more.

ENS: This system does not store, process, or disseminate sensitive or PII data.

(c) Any information sharing conducted by the system:

WebTA: The information collected is shared with NFC's automated personnel/payroll processing system.

COOP-WB: The information collected is shared internally among agency emergency management personnel, COOP Business Unit managers/assistants, and USPTO Senior Management.

ENS: This system does not store, process, or disseminate sensitive or PII data.

(d) A citation of the legal authority to collect PII and/or BII:

WebTA: PII information is initially collected during the employment application process and is further used by and contained within WebTA to process time and attendance data. The Office of Personnel Management (OPM) is authorized to request PII information for the purpose of Federal and Federal contract employment under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U.S. Code. Section 1104 of title 5 allows OPM to delegate personnel management functions to other Federal agencies.

COOP-WB: The information collected is provided voluntarily and by manual input from emergency management personnel, COOP Business Unit Managers/assistants, and USPTO Senior Management. This information is collected under Federal Continuity Directive-1 (FCD-1), January 2017. It is necessary to collect such information from essential personnel because their roles and responsibilities align to emergency management duties.

ENS: This system does not store, process, or disseminate sensitive or PII data.

(e) The Federal Information Processing Standard (FIPS) 199 security impact category for the system

WebTA, COOP-WB, & ENS: The Sub-system security impact category is Moderate.

CAOS: The Master System high water-mark security impact category is 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.)*
- This is an existing information system in which changes do not create new privacy risks. *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):					

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*	<input checked="" type="checkbox"/>	e. File/Case ID	<input type="checkbox"/>	i. Credit Card	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input checked="" type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form: WebTA collects and maintains USPTO employee Social Security Numbers (SSN) to process personal leave balances, time and attendance (T&A) information, employee information, and position description. The T&A information are transmitted to NFC for payroll process using SSN from both WebTA and NFC for identification.					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished: No, there is no way to avoid future collection of SSN. WebTA utilizes SSNs to ensure each employee is associated to a unique identifier and allows for accurate processing of payroll transactions.					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input type="checkbox"/>	n. Financial Information	<input type="checkbox"/>
c. Alias	<input checked="" type="checkbox"/>	i. Home Address	<input checked="" type="checkbox"/>	o. Medical Information	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	j. Telephone Number	<input checked="" type="checkbox"/>	p. Military Service	<input checked="" type="checkbox"/>

e. Age	<input type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	l. Education	<input type="checkbox"/>	r. Mother's Maiden Name	<input type="checkbox"/>
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	<input checked="" type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>	g. Salary	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>	h. Work History	<input type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input type="checkbox"/>		
i. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input checked="" type="checkbox"/>
j. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input checked="" type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
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	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input type="checkbox"/>	Email	<input type="checkbox"/>		
Other (specify):					

Government Sources					
Within the Bureau	<input checked="" type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

Non-government Sources					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application			<input type="checkbox"/>		
Other (specify):					

- 2.3 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	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	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			
To determine eligibility	<input type="checkbox"/>	For administering human resources programs	<input checked="" type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input type="checkbox"/>
For web measurement and customization technologies (single-session)	<input type="checkbox"/>	For web measurement and customization technologies (multi-session)	<input type="checkbox"/>
Other (specify): WebTA collects and maintains USPTO employee Social Security numbers to process, personal leave balances; time and attendance information, employee related information, position description and management information. For COOP-WB , Individual COOP officers in the various major Offices and Business Units within USPTO supply information and requirements supporting emergency Continuity of Operations for the USPTO. COOP-WB collects the necessary staff/employee resource information such as: names, personal home number, personal cell number, and personal email.			

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).

WebTA captures employee Social Security Numbers in order to collect, validate, and electronically certify time and attendance information. This information is further collected for secure transmission over the USPTO network to the National Finance Center (NFC) for payroll processing. WebTA collects only USPTO employee information.

The COOP-WB information is to be used only in reporting to the COOP Manager and USPTO Senior Management, and creation of the overall USPTO COOP Workbook. COOP-WB collected information is used to support emergency Continuity of Operations for the USPTO. Both USPTO employee and contractor information is collected from those personnel with emergency Continuity of Operations responsibilities.

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	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The PII/BII in the system will not be shared.

6.2 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:

	<p>WebTA interconnects with the Department of Agriculture’s National Finance Center (NFC) for payroll processing. All data transmissions require credential verification and validation of data prior to transmitting. The data passes through a dedicated interconnection (IPSec VPN tunnel) established with NFC.</p> <p>COOP-WB information will be shared internally to the COOP Office and with USPTO Senior Management (via reports and the overall Workbook). COO-WB information is protected within USPTO’s secure perimeter through the Network and Security Infrastructure (NSI) system.</p>
<input type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input checked="" type="checkbox"/>		
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.*)

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
<input checked="" type="checkbox"/>	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: CAOS: https://www.opm.gov/forms/pdf_fill/of0306.pdf and USPTO’s internal IT Privacy Policy (<i>for business use only</i>). COOP-WB: USPTO’s internal IT Privacy Policy (<i>for business use only</i>).	
<input type="checkbox"/>	Yes, notice is provided by other means.	Specify how:
<input type="checkbox"/>	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: CAOS: PII data is collected as part of the employment process through OMB Form 3206-0182. Applicants can decline to provide their information, however, in doing so, the agency and federal government would not be able to process their employment application.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: CAOS: PII data is collected as part of the employment process through OMB Form 3206-0182. General or routine uses of the information collected is disclosed in the Form. Applicants can decline to provide their information, however, in doing so, the agency and federal government would not be able to process their employment application.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: CAOS: USPTO employees have the opportunity to review and update their personal information online through NFC's Employee Personal Page application or the Department of Treasury's HR Connect system. Employees may also visit the USPTO's Office of Human Resources (OHR) department for additional assistance.
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Unauthorized access, suspicious system log behavior and log failures are audited in real time and reported to the appropriate personnel to troubleshoot and remediate any potential issues.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 10/2/2016 <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	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 (POAM).
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts

	required by DOC policy.
<input type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

In accordance with NIST 800-18 Rev. 1 and NIST 800-53 Rev. 4, the CAOS 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. The SSP is reviewed on an annual basis. In addition, annual assessments and Continuous Monitoring reviews are conducted on the CAOS data. The USPTO Office of Policy and Governance/Cybersecurity Division (OPG/CD) conducts these assessments and reviews based on NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53A Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations. The results of these assessments and reviews are documented in the CAOS Security Assessment Package as part of the system's Security Authorization process.

Management Controls

1. USPTO uses the Life Cycle review process to ensure that management controls are in place for CAOS. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan. The System Security Plan specifically addresses the management, operational, and technical controls that are in place, and planned, during the operation of the enhanced system. Additional management controls include performing national agency checks on all personnel, including contractor staff. Additionally, USPTO develops privacy and PII-related policies and procedures to ensure safe handling, storing, and processing of sensitive data.

Operational Controls

1. Automated operational controls include securing all hardware associated with the CAOS in the USPTO Data center. The Data Center is controlled by access card entry, and is manned by a uniformed guard service to restrict access to the servers, their Operating Systems and databases. Contingency planning has been prepared for the data. Backups are performed on the processing databases. Backups are stored on tape and are secured off-site. Additional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.

2. Manual procedures shall be followed for handling extracted data containing sensitive PII, which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:

- a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
- b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.
- c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
- d. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private Network (VPN).
- e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

Technical Controls

1. CAOS is secured by various USPTO infrastructure components, including the Network and Security Infrastructure (NSI) system and other OCIO established technical controls to include password authentication at the server and database levels. Web communications leverages modern encryption technology such as TLS 1.1/1.2 over HTTPS. Dedicated interconnections offer protection through IPsec VPN tunnels.

Section 9: Privacy Act

9.1 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.”

<input checked="" type="checkbox"/>	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>):</p> <p>Records contained in these systems do not constitute a new system of records within the meaning of the Privacy Act. The following are existing SORNs:</p> <p>CAOS: The existing system of records covers the information residing in the database. These include: <i>COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.</i></p> <p>COOP: The existing system of records covers the information residing in the database. These include: <i>COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.</i></p>
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	No, a SORN is not being created.

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.*)

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule:
<input checked="" type="checkbox"/>	USPTO Office of the Chief Administrative Officer Comprehensive Records Schedule 2016: http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/docs/Section%208-%20Office%20of%20the%20Chief%20Administrative%20Officer.pdf
<input type="checkbox"/>	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:
<input checked="" type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify): PII collected by COOP-WB is disposed when it is no longer valid using above mentioned methods. The PII collected by WebTA is not disposed.			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels

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.

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	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 levels.
(Check all that apply.)

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: PII stored in the system is data collected from USTPO employees and contractor personnel in which the information is confidential and unique to those individuals. The unauthorized access, modification, and/or disclosure of sensitive data would have a Moderate impact on the organization and its operations.
<input type="checkbox"/>	Other:	Provide explanation:

Section 12: Analysis

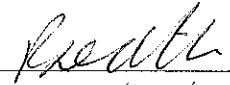

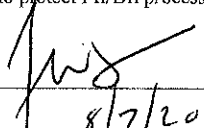
12.1 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.

USPTO Points of Contact and Signatures

<p>System Owner Name: Colleen Sheehan Office: 600 Dulany Street, Elizabeth Townhouse, Room 4A09, Alexandria, VA 22314 Phone: 571-272-8246 Email: Colleen.Sheehan@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p style="text-align: right;">Users, Sheehan, <small>Digitally signed by Users, Sheehan, Colleen DN: dn=go, dc=uspto, cn=Users, o=Sheehan, Colleen Date: 2017.08.01 16:03:02 -04'00'</small></p> <p>Signature: <u>Colleen</u></p> <p>Date signed: <u>08/01/2017</u></p>	<p>Senior Information Security Officer Name: Rami Dillon Office: 600 Dulany Street, Madison West, Room 05C07, Alexandria, VA 22314 Phone: 571-272-8233 Email: Rami.Dillon@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u></u></p> <p>Date signed: <u>8/2/17</u></p>
<p>Bureau Chief Privacy Officer and Co-Authorizing Official Name: John B. Owens II Office: 600 Dulany Street, Madison East, Room 10D15, Alexandria, VA 22314 Phone: 571-272-9400 Email: John.Owens@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u></u></p> <p>Date signed: <u>8/3/17</u></p>	<p>Co-Authorizing Official Name: Frederick Steckler Office: 600 Dulany Street, Madison West, Room 10A15, Alexandria, VA 22314 Phone: 571-272-9600 Email: Frederick.Steckler@uspto.gov</p> <p>I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.</p> <p>Signature: <u></u></p> <p>Date signed: <u>8/7/2017</u></p>

****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.****