Version Number: 01-2017

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

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

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

Jennifer Goode 03/22/2021

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

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

(b) System location

The CAOS system resides at the USPTO facilities located in Alexandria, Virginia.

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

CAOS interconnects with following other systems:

Enterprise Unix Services (EUS)
Enterprise Windows Servers (EWS)
Information Delivery Product (IDP)
Service Orientated Infrastructure (SOI)
Corporate Web Systems(CWS)
Database Services (DBS)
Enterprise Software Services (ESS)
Network and Security Infrastructure (NSI)
Enterprise Monitoring and Security Operations (EMSO)

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

Web Time and Attendance Automated System (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.

Continuity of Operations Plan Work Book (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.

Emergency Notification System (ENS) collects and maintains USPTO employee ID, email ID, work and home phone number, work and home address which 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.

Record Sharing Platform (RSP) application presents USPTO employee ID, log in/log out, badge in/badge out details in report format which enables the USPTO supervisors and business unit managers to verify the information that is being entered into the USPTO WebTA time reporting system.

Enterprise Telework Information System (ETIS) collects and maintains USPTO employee ID, email ID, work and home phone number, work and home address/alternative telework address for administering Telework programs

(e) How information in the system is retrieved by the user

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: The USPTO Emergency Notification System (ENS) provides rapid dissemination of emergency messages to USPTO personnel and contractors via desktop notifications on and mail messages to USPTO email accounts. Also, ENS provides a "Self Service" facility where users may provide additional mean of contact, such as Cell, Home phone or alternate email which will also receive the alert.

RSP: RSP is used by USPTO employees to view, through a user interface, their badge in/badge out and log in/log out details.

ETIS: ETIS is used by all USPTO Business Units (other than Patents) and offers an easy-to-update pop-up of employee information, including employee telework applications; seamless communication with HR systems, and history/version controls to track data.

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

The information is transmitted to and from the CAOS system using end-to-end secure transport layer protocols.

(g) 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**:** The information collected is shared internally among agency emergency management personnel.

RSP: Information hosted or collected by RSP is only accessible to individual users and RSP administrators and is not shared with anyone else within USPTO or outside USPTO.

ETIS: Information hosted or collected by ETIS is only accessible to respective USPTO business units (except Patents) and its employees. The information is not shared with anyone outside USPTO.

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

The information is collected for the purpose of Federal and Federal contract employment under sections 1302, 3301, 3304, 3328, and 8716 of title 5; Executive Order 9397, as amended; and U.S. Code and Federal Continuity Directive-1 (FCD-1). Section 1104 of title 5 allows OPM to delegate personnel management functions to other Federal agencies.

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

WebTA, COOP-WB, RSP, ENS and ETIS: 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.)*

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 (version 01-2015).

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2017 or later).

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:

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. 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	☒	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. Physical Characteristics	☐
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	☐		
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	☐		
k. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	☐	d. Photographs	☐	g. DNA Profiles	☐
b. Palm Prints	☐	e. Scars, Marks, Tattoos	☐	h. Retina/Iris Scans	☐
c. Voice Recording/Signatures	☐	f. Vascular Scan	☐	i. Dental Profile	☐
j. 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	☒	d. 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.

All System related generic error messages are presented to users while detailed debugging error messages are provided to administrators. Error conditions are handled so as not to provide information that could be exploited by adversaries. Access to the system is only assigned to authorized users with specific role based restrictions, and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The USPTO maintains an audit trail and performs random periodic reviews to identify unauthorized access.

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.
☒	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):			

☒	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).

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.
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.
ENS collected information 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. Both USPTO employee and contractor information is originally collected from those personnel at the time of onboarding.
ETIS collects PII, such as name, home address, and telephone number of USPTO employees and public data, such as work ID, location, email, telephone number, etc, to file and manage telework applications.
RSP application uses USPTO employee ID, log in/log out, badge in/badge out details and presents it in report format which enables the USPTO supervisors and business unit managers to verify the information that is being entered into the USPTO WebTA time reporting system.

5.2 Describe any potential threats to privacy 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.)

The scope of potential threat to privacy is internal to USPTO. CAOS implements security and management controls to prevent the inappropriate disclosure of sensitive information. Management controls are utilized to prevent the inappropriate disclosure of sensitive information including Annual Security Awareness Training which is mandatory for all USPTO employees. It includes training modules on understanding privacy responsibilities and procedures and other information such as defining PII and how it should be protected. Security controls are employed to ensure information is resistant to tampering, remains confidential as necessary, and is available as intended by the agency and expected by users. USPTO implements automatic purging of information, as applicable, by means of deletion and/or shredding. In addition, the Perimeter Network (NSI) and EMSO provide additional automated transmission and monitoring mechanisms to ensure that PII information is protected and not breached by any outside entities.

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 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: **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. **COOP-WB** information will be shared internally to the COOP Office and with USPTO Senior Management (via reports and the overall Workbook).COOP-WB information is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) system. **ENS** information will be shared internally to the agency emergency management personnel and with USPTO Senior Management. ENS information is protected within USPTO's secure perimeter through The Network and Security Infrastructure (NSI) system. **ETIS** information will be shared internally to the ETIS management personnel and with USPTO Senior Management. ETIS information is protected within USPTO's secure perimeter through the Network and Security Infrastructure (NSI) system. **RSP** information will be shared internally to the Human Resources management personnel and with USPTO Senior Management. R information is protected within USPTO's secure perimeter through The Network and Security Infrastructure (NSI) system.
☐	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	☐	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: **CAOS:** https://www.opm.gov/forms/pdf_fill/of0306.pdf and USPTO's internal IT Privacy Policy (*for business use only*).	
☐	Yes, notice is provided by other means.	Specify how:
☐	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: **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. **ETIS:** In addition to PII data collected as part of the employment process, applicants are requested to provide alternate work location address and alternate work phone number. 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.
☐	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: **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. **ETIS:** In addition to PII data collected as part of the employment process, applicants are requested to provide alternate work location address and alternate work phone number. 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.
☐	No, individuals do not have an opportunity to consent to particular	Specify why not:

	uses of their PII/BII.	

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: **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. **ETIS:** ETIS users have the opportunity to review and update their personal information online through ETIS application.
☐	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: 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.
☒	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 12/09/20 ☐ 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 supporting 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 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).*

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 User ID; (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.
2. Also, ETIS leverages Microsoft .NET framework (CLR assembly) in SQL Server 2017 for encryption/decryption of PII data at rest. In addition, the application follows the principle of least privilege with proper user roles to ensure the users only access the information and resources that are necessary for their needs.

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."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number *(list all that apply)*: COMMERCE/DEPT-25, Access Control and Identity Management System. **ENS:** An existing system of records notice covers the information residing in the database: COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies. **COOP:** An existing system of records notice covers the information residing in the database: COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies. **WebTA:** An existing system of records notice covers the information residing in the database: COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons. **ETIS:** An existing system of records notice covers the information residing in the database: COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.
☐	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: USPTO Office of the Chief Administrative Officer Comprehensive Records Schedule 2018
☐	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): PII collected by COOP-WB, ETIS and ENS 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.
(The PII Confidentiality Impact Level is not 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 levels. *(Check all that apply.)*

☒	Identifiability	Provide explanation: PII stored in the system is data collected from USPTO 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.
☒	Quantity of PII	Provide explanation: PII stored in the system is data collected from USPTO 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.
☒	Data Field Sensitivity	Provide explanation: PII stored in the system is data collected from USPTO 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.
☒	Context of Use	Provide explanation: PII stored in the system is data collected from USPTO 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.
☒	Obligation to Protect Confidentiality	Provide explanation: PII stored in the system is data collected from USPTO 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.
☒	Access to and Location of PII	Provide explanation: PII stored in the system is data collected from USPTO 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.
☐	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 scope of potential threat to privacy is internal to USPTO. Management controls are utilized to prevent the inappropriate disclosure of sensitive information including Annual Security Awareness Training which is mandatory for all USPTO employees. It includes

Security Awareness Training which is mandatory for all USPTO employees. It includes training modules on understanding privacy responsibilities and procedures and other information such as defining PII and how it should be protected.

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.