

**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

CHARLES CUTSHALL

Digitally signed by CHARLES CUTSHALL
Date: 2025.02.27 14:09:16 -05'00'

2/27/2025

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: CAOS-005-00

Introduction: System Description

Provide a brief description of the information system.

The Corporate Administrative Office System (CAOS) – is an information system that is composed of 3 components that support the Human Resources business functions within the United States Patent and Trademark Office (USPTO).

Enterprise Telework Information System (ETIS) – enables eligible USPTO employees to manage the information about their primary and secondary telework sites. USPTO employee supervisors use this to review and approve employee telework sites.

Record Sharing Platform (RSP) – is an auditing system that allows USPTO employees and management to verify the information employees enter into WebTA.

WebTA – allows USPTO employees to manage their time and attendance and manage their leave.

Address the following elements:

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

CAOS is a major application.

(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 and the sub-components ETIS and RSP interconnect with:

- **ICAM-Identity as a Service (ICAM-IDaaS):** provides an enterprise authentication and authorization service for USPTO applications.

Additionally, CAOS and all of its sub-components interconnect to:

- **Corporate Web Systems (CWS):** is a platform that provides web browser access to CAOS and its sub-components.
- **Enterprise Software Services (ESS):** provides a variety of support services necessary for CAOS and its sub-components.
- **Enterprise Unix Services (EUS):** provides Operating System (OS) support services for CAOS component servers.
- **Enterprise Windows Servers (EWS):** provides OS support services for CAOS component servers Incorporated.
- **Information Delivery Product (IDP):** is a platform that provides data feeds to CAOS components WebTA, ETIS, and RSP.
- **Network and Security Infrastructure (NSI):** facilitates the communications, secure access, protective services, and network infrastructure support for all CAOS Components.
- **Database Services (DBS):** provides database management services for all CAOS components.
- **Security and Compliance Services (SCS):** provides Security, compliance and monitoring services for all CAOS components.
- **Storage Infrastructure Managed Service (SIMS):** provides and maintains storage for all CAOS components.
- **Service Oriented Infrastructure (SOI):** provides a feature-rich and stable platform upon which CAOS component applications can be deployed.

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

ETIS – enables eligible USPTO employees to manage the information about their primary and secondary telework sites. USPTO employee supervisors use this to review and approve employee telework sites. Employees enter telework locations and are able to make telework address changes and submit changes to telework programs for approval within the system.

RSP – is an auditing system that allows USPTO employees and management to verify the information employees enter into WebTA, from a log-in and log-out, work hours perspective. Employees can log into RSP and review log-in, log-out times or badge in, badge out times. PII is limited to name, employee ID that is received from data feed.

WebTA – USPTO employees log-in to WebTA with their username and password. The employee can enter their hours worked into the appropriate timecode and validate their timesheet

for supervisory approval for each pay period. Additionally, the employee can submit their leave request into the system. The employee's supervisor is required to log-in WebTA and certify an employee's timesheet and approve their leave request. The employee and supervisor are able to view the historical timecards, as needed as far back as 2006. In addition to USPTO employees and their supervisors having access to the employee's timesheet, a timekeeper also has access and is able to validate an employee's sheet on their behalf if they are on leave and enable timecodes for employees.

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

ETIS: is used by all USPTO Business Units.

- **Telework Applicants and Participants** can view their own employee and telework data by accessing the system under Single Sign On (SSO). The users have the option in the User Interface (UI) to view their telework history, current telework agreement, and any of their own pending telework applications or change requests.
- **Non-Patents Telework Approvers** are only able to view and act on the employee and telework information of the employees for whom they are an approver or delegate approver. They have the option in the UI to view employee telework history, current telework agreements, and pending telework applications and change requests.
- **Non-Patents Telework Coordinators** are only able to view the employee and telework information of the employees in their own Business Unit using the Participants Report, available to them on the UI.
- **Patents Telework Coordinators** are also approvers. They can view and act on the employee and telework information of the Patents employees for whom they have been given approver rights. They can also view Patents employee and telework information using the Participants Report, available to them on the UI.
- **Patents Supervisors** are not approvers, but they can view the employee and telework information of their direct reports by the UI "My Employees" tab.
- **Telework Program Office** specialists and delegates can view the employee and telework information of all USPTO employees using the Participants Report, available to them on the UI.

RSP: is used by USPTO employees to view, through a user interface, their badge in/badge out (BIBO), and log in/log out (LILO) details. Employees have a User Interface which allows access to their badge in/badge out and log in/log out information. System Admins and System Owners have a User Interface which allow them to see employee BIBO/LILO information.

WebTA: Allows USPTO employees to view, record, track, validate and certify their time and attendance and leave 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

WebTA: The information collected is shared with NFC's automated personnel/payroll processing system. The information is extracted out of WebTA and transmitted to Department of Agriculture NFC personnel/payroll system via a VPN using Internet Protocol Security (IPsec) security. No direct connection between WebTA and NFC.

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

5 U.S.C. 1104, 5 U.S.C. 301, 35 U.S.C. Part I, 5 USC 6501 et seq.
General Accounting Office-03-352G, Maintaining Effective Control Over Employee Time and Attendance Reporting;
5 CFR Part 550, Pay Administration
5 CFR Part 630, Absence and Leave
41 CFR Part 102-74, Subpart F. Telework
E.O. 9397;
DAO 205-16 management of electronic records

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

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

- ☐ This is a new information system.
- ☐ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)

a. Conversions	<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):					

☒ 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*	<input checked="" type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>	m. Medical Record	<input type="checkbox"/>
e. File/Case ID	<input type="checkbox"/>				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form: SSN is used to ensure accurate employee reporting and is a required unique identifier for NFC.					

General Personal Data (GPD)					
a. Name	<input checked="" type="checkbox"/>	h. Date of Birth	<input type="checkbox"/>	o. Financial Information	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	i. Place of Birth	<input type="checkbox"/>	p. Medical Information	<input type="checkbox"/>
c. Alias	<input checked="" type="checkbox"/>	j. Home Address	<input checked="" type="checkbox"/>	q. Military Service	<input type="checkbox"/>
d. Gender	<input type="checkbox"/>	k. Telephone Number	<input checked="" type="checkbox"/>	r. Criminal Record	<input type="checkbox"/>
e. Age	<input type="checkbox"/>	l. Email Address	<input checked="" type="checkbox"/>	s. Marital Status	<input type="checkbox"/>
f. Race/Ethnicity	<input type="checkbox"/>	m. Education	<input type="checkbox"/>	t. Mother's Maiden Name	<input type="checkbox"/>
g. Citizenship	<input type="checkbox"/>	n. Religion	<input type="checkbox"/>		
u. Other general personal data (specify):					

Work-Related Data (WRD)

a. Occupation	<input checked="" type="checkbox"/>	e. Work Email Address	<input checked="" type="checkbox"/>	i. Business Associates	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	f. Salary	<input type="checkbox"/>	j. Proprietary or Business Information	<input type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	g. Work History	<input type="checkbox"/>	k. Procurement/contracting records	<input type="checkbox"/>
d. Work Telephone Number	<input checked="" type="checkbox"/>	h. Employment Performance Ratings or other Performance Information	<input type="checkbox"/>		
l. Other work-related data (specify): WebTA records include individuals taking sick leave or Family and Medical Leave Act (FMLA).					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	<input type="checkbox"/>	f. Scars, Marks, Tattoos	<input type="checkbox"/>	k. Signatures	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	g. Hair Color	<input type="checkbox"/>	l. Vascular Scans	<input type="checkbox"/>
c. Voice/Audio Recording	<input type="checkbox"/>	h. Eye Color	<input type="checkbox"/>	m. DNA Sample or Profile	<input type="checkbox"/>
d. Video Recording	<input type="checkbox"/>	i. Height	<input type="checkbox"/>	n. Retina/Iris Scans	<input type="checkbox"/>
e. Photographs	<input type="checkbox"/>	j. Weight	<input type="checkbox"/>	o. Dental Profile	<input type="checkbox"/>
p. 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"/>	f. 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 Describe how the accuracy of the information in the system is ensured.

<p>Information required for CAOS and its components is provided by the employee during the start of employment. Users can review and update their information in consultation with the Office of Human Resources.</p> <p>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.</p>

2.4 Is the information covered by the Paperwork Reduction Act?

<input type="checkbox"/>	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
<input checked="" type="checkbox"/>	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	<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			
For a Computer Matching Program	<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):			

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).

ETIS PII that is collected pertains only to federal employees. 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 PII that is collected pertains to federal employees and contractors. The 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. PII is limited to employee name and employee ID.

WebTA PII that is collected pertains only to federal employees. 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 NFC for payroll processing. WebTA collects only USPTO employee information. PII also includes name and employee ID.

- 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.)

The scope of potential threat to privacy within the CAOS system are insider threats, foreign and adversarial entities. 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 SCS provide additional automated transmission and monitoring mechanisms to ensure that PII information is protected and not breached by any outside entities.

Information Delivery Product (IDP): System that provides employee data feeds to CAOS components ETIS, WebTA and RSP. The data is transmitted via secure network protocols and encryption of data in transit and at rest.

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 checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input checked="" type="checkbox"/>	<input checked="" 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"/>

<input type="checkbox"/>	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?

<input checked="" type="checkbox"/>	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
<input type="checkbox"/>	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.

<input checked="" type="checkbox"/>	<p>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: ICAM-IDaaS ESS IDP SCS</p> <p>Information Delivery Product (IDP): System that provides employee data feeds to CAOS components ETIS, WebTA and RSP. The data is transmitted via secure network protocols and encryption of data in transit and at rest.</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.

6.4 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	<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> .	
<input checked="" type="checkbox"/>	Yes, notice is provided by other means.	Specify how: This PIA serves as a nother notice
<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 type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals do not have the opportunity to decline to provide PII/BII into CAOS. The data within the system is required as a part of business operations. USPTO Employees can choose not to provide a telework location but then are not a ble to participate in the telework program. Alternative contact information for emergency notices is the choice of the individual.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals do not have the opportunity to consent to particular uses of their PII/BII, as the requested PII/BII is necessary for the system to complete its purpose.

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 ETIS component: Individuals have the opportunity to review and update their personal information online through ETIS application.
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: WebTA and RSP: USPTO employees are unable to update their PII directly within WebTA or RSP however they 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.

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: Application, System and Security logs are used to track and record access to PII/BII.
<input checked="" type="checkbox"/>	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): 9/29/2023 <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 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
<input checked="" type="checkbox"/>	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
<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 DOC 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.
(Include data encryption in transit and/or at rest, if applicable).

In accordance with NIST 800-18 and NIST 800-53, the CAOS System Security and Privacy Plan (SSPP) 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 SSPP is reviewed on an annual basis. In addition, annual assessments and Continuous Monitoring reviews are conducted on the CAOS data. The USPTO Cybersecurity Assessment and Authorization Branch (CACB) conducts these assessments and reviews based on NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-53, 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

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 SSPP. The SSPP 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

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.

Manual procedures are 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:

- 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.

- 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.
- Obtain management concurrence in the log, if an extract aged over 90 days is still required.
- 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 VPN.
- Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as Compact Disc (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 Transport Layer Security (TLS) 1.1/1.2 over Hypertext Transfer Protocol Secure (HTTPS). Dedicated interconnections offer protection through IPsec Virtual Private Network (VPN) tunnels.

2. Also, ETIS leverages Microsoft .NET framework (CLR assembly) in Structured Query Language (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 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.”

<input checked="" type="checkbox"/>	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. <i>(list all that apply):</i></p> <p>COMMERCE/DEPT-25, Access Control and Identity Management System. COMMERCE/DEPT-1, Attendance, Leave, and Payroll Records of Employees and Certain Other Persons. COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies. PAT-TM-16, USPTO PKI Registration and Maintenance System. PAT-TM-17, USPTO Security Access Control and Certificate Systems. PAT-TM-18, USPTO Personal Identification Verification (PIV) and Security Access Control Systems.</p>
<input type="checkbox"/>	Yes, a SORN has been submitted to the Department for approval on <u>(date)</u> .
<input type="checkbox"/>	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.)*

<input checked="" type="checkbox"/>	<p>There is an approved record control schedule. Provide the name of the record control schedule:</p> <p>GRS 2.4, item 030, Time and Attendance Records GRS 2.4, item 040, Agency payroll record for each pay period GRS 2.3, item 040, Telework/alternate worksite program case files GRS 5.3, item 010, Continuity planning and related emergency planning files GRS 5.3, item 020, Employee emergency contact information GRS 5.1, item 020, Non-recordkeeping copies of electronic records GRS 2.4, item 060, Payroll program administrative records; Administrative correspondence between agency and payroll processor, and system reports used for agency workload and or personnel management purposes GRS 2.4, item 061, Payroll program administrative records; Payroll system reports providing fiscal information on agency payroll GRS 5.7, item 050, Mandatory reports to external Federal entities regarding administrative matters GRS 3.1, item General Technology Management Records - Information technology operations and maintenance records. -system logs. GRS 4.2, item 140, Information Access and Protection Records-Personally identifiable information extract logs.</p>
<input type="checkbox"/>	<p>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:</p>
<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 type="checkbox"/>	Overwriting	<input type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
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.)*

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

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: The combination of the above PII such as SSN, name, financial account etc., can readily identify a particular individual.
<input checked="" type="checkbox"/>	Quantity of PII	Provide explanation: The PII stored in the system consists of all employees and contractors and is in the tens of thousands.
<input checked="" type="checkbox"/>	Data Field Sensitivity	Provide explanation: The combination of the PII stored in the systems together makes the data fields more sensitive.
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: The data in the system is used to process personal leave balances, time and attendance information, employee information and position description.
<input checked="" type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation: Based on the data collected USPTO must protect the PII of each individual in accordance to the Privacy Act of 1974.
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Because the information containing PII must be transmitted outside of the USPTO environment, there is an added need to ensure the confidentiality of information during

		transmission. Necessary measures must be taken to ensure the confidentiality of information during processing, storing and transmission.
<input type="checkbox"/>	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 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.

<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.

- 12.3 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.