Template Version Number: 01-2021

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

Privacy Threshold Analysis
for the
Corporate Administrative Office System (CAOS)

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Corporate Administrative Office System (CAOS)

Unique Project Identifier: **EBPL-CAOS-005-00**

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system: *Provide a brief description of the information system.*
The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

The Corporate Administrative Office System (CAOS) is an information system. The purpose of the CAOS is to support the Human Resources business functions within the United States Patent and Trademark Office (USPTO).

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 interconnects with following other systems:

- **Corporate Web Systems (CWS):** The Corporate Web System (CWS) is an n-tier application architecture that consists of www.uspto.gov, PTOWeb, RDMS, and Image Gallery. The web servers are responsible for accepting HTTP requests from web clients and passing the requests to the application servers. All hardware components and operating systems supporting the CWS are managed as part of the USPTO Enterprise UNIX Servers (EUS), Service Oriented Infrastructure (SOI), Database Services (DBS), and Network Security Infrastructure (NSI) systems. The CWS provides a feature-rich and stable platform that contains the Organization's Websites that are used at USPTO such as Intranet and USPTO external website.

- **Database Services (DBS):** The Database Services Branch (DSB) manages and maintains database management software installed on enterprise and application servers. They perform database control and administration functions associated with database operations, performance, and integrity. Support services are also provided for developing Automated Information Systems (AISs) such as requirements analysis, database design, and implementation and maintenance strategies of database applications.

- **Enterprise Software Services (ESS):** ESS is comprised of multiple on premise and in-the-cloud software services, which support the USPTO in carrying out its daily tasks. Within this system, the services are broken up into several subsystems. These subsystems are Enterprise Active Directory Services (EDS), MyUSPTO, Role Based Access Control (RBAC), Email as a Service (EaaS), Enterprise SharePoint Services (ESPS), Symantec Endpoint Protection, and PTOFAX.

- **Enterprise Unix Services (EUS):** The Enterprise UNIX Services (EUS) is a General Support System with a purpose of providing a LINUX base hosting platform to support other information systems at USPTO. The system supports the underlying operating system, OS patching and updates, and OS level baseline compliance.

- **Enterprise Windows Servers (EWS):** The Enterprise Windows Services (EWS) is an Infrastructure information system, and provides a basic hosting platform for major applications that support various USPTO missions. Data is generally owned by the application not the platform. The USPTO facilities are leased by the General Services Administration (GSA) from LCOR, Incorporated. The facility that houses the EWS components is equipped with physical and environmental protective measures that ensure ongoing operation.

- **Information Delivery Product (IDP):** IDP is a Master System composed of the following three (3) subsystems: 1) Enterprise Data Warehouse (EDW), 2) Electronic Library for Financial Management System (EL4FMS), and 3) Financial Enterprise Data Management Tools (FEDMT).

- **Security and Compliance Services (SCS):** SCS provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

- **Service Oriented Infrastructure (SOI):** SOI provides a feature-rich and stable platform upon which USPTO applications can be deployed.

- **Network and Security Infrastructure (NSI):** The NSI facilitates the communications, secure access, protective services, and network infrastructure support for all USPTO applications.

d) The purpose that the system is designed to serve

The purpose of the CAOS is to support the Human Resources business functions within USPTO. The CAOS supports all activities associated with the recruitment and management of USPTO personnel. The CAOS is composed of five Information Systems 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.
- Used by employees to view, through a user interface, their badge in/badge out and log in/log out details.
- Store and maintain all information required to monitor the USPTO Telework Program.

e) *The way the system operates to achieve the purpose*

Continuity of Operations Plan Work Book (COOP- WB) is 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 reduces the amount of time agency continuity personnel spend completing the Business Continuity and Contingency Plan (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, whether those failures occur in an automated information system or in a particular building. This should provide critical data/information to the agency during a continuity event and could decrease the amount of time needed to return the agency to full operational status.

Emergency Notification System (ENS) is a network-based application that provides rapid dissemination of emergency messages to USPTO personnel through an audible alert and visual desktop popup text message. 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. It is a rapid and effective means of notifying the entire USPTO community (10,000+ employee workstations) in less than five minutes so they may react quickly in an emergency. This includes those working from a remote location (teleworking) as well as those on campus.

Enterprise Telework Information System (ETIS) is an application system for the Non-Patents Telework System Database that can store and maintain all information required to monitor the USPTO Telework Program. This web-based database is accessible to all 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. The Telework System Database also has filtering capabilities and easy to develop dashboard and canned reports for a system administrator. Lastly, the database has workflow management that allows for the submission of new electronic telework applications, notifications and reminders throughout the telework approval chain, and prompts of required information to complete an application or change. The information being housed contains information about teleworking employees in all Business Units outside of Patents.

Record Sharing Platform (RSP) is used by employees to view, through a user interface, their badge in/badge out and log in/log out details. The information that is contained within the Record Sharing Platform system enables a user to verify the information that is being entered into the USPTO WebTA time reporting system. RSP is not a system of records.

Web Time and Attendance Automated System (WebTA) allows USPTO time and attendance (T&A) 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.

f) A general description of the type of information collected, maintained, used, or disseminated by the system

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.

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.

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.

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.

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.

g) Identify individuals who have access to information on the system

COOP-WB: COOP Staff and System Administrators.

ENS: All USPTO Employees and Contractors.

ETIS: Super System Administrator, System Administrator - Business Unit, Approver, Approver – Reports, Participants, and Applicants.

RSP: Employees, Supervisors, Delegated Supervisors, Business Administrator (BA), and Technical Administrators.

WebTA: USPTO Employees (End users), OHR, Supervisors, Administrators, and Timekeepers have access.

h) How information in the system is retrieved by the user

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.

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.

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

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.

i) 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

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. *Continue to answer questions and complete certification.*

☒ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment. *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

☐ Yes. This is a new information system.

☐ Yes. This is an existing information system for which an amended contract is needed.

☐ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

☒ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?
NIST Special Publication 800-53 Revision 4, Appendix J, states " Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ Yes. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify):			

☒ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?
As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII.

☒ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?
As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

☒ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

☒ DOC employees
☒ Contractors working on behalf of DOC
☐ Other Federal Government personnel
☐ Members of the public

☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

☒ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, 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. WebTA utilizes SSNs to ensure each employee is associated to a unique identifier and allows for accurate processing of payroll transactions.

Provide the legal authority which permits the collection of SSNs, including truncated form.

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 employment 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. Executive Order 9397, as amended, also provided authority for the collection of SSNs.

☐ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

☒ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

☐ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

☒ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

☐ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ The criteria implied by one or more of the questions above **apply** to the Corporate Administrative Office System (CAOS) and as a consequence of this applicability, a PIA will be performed and documented for this IT system.

☐ The criteria implied by the questions above **do not apply** to the Corporate Administrative Office System (CAOS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

System Owner Name: Sheehan Colleen Office: Office of Human Resources (OHR) Phone: (571) 272-8246 Email: Colleen.Sheehan@uspto.gov Signature: Users, Sheehan, Colleen Digitally signed by Users, Sheehan, Colleen Date: 2023.03.15 16:35:23 -04'00' Date signed: ______________________________	**Chief Information Security Officer** Name: Don Watson Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-8130 Email: Don.Watson@uspto.gov Signature: Users, Watson, Don Digitally signed by Users, Watson, Don Date: 2023.03.15 20:21:27 -04'00' Date signed: ______________________________
Privacy Act Officer Name: Ezequiel Berdichevsky Office: Office of General Law (O/GL) Phone: (571) 272-1557 Email: Ezequie.Berdichevsky@uspto.gov Signature: Users, Berdichevsky, Ezequiel Digitally signed by Users, Berdichevsky, Ezequiel Date: 2023.03.14 09:31:19 -04'00' Date signed: ______________________________	**Bureau Chief Privacy Officer and Co-Authorizing Official** Name: Henry J. Holcombe Office: Office of the Chief Information Officer (OCIO) Phone: (571) 272-9400 Email: Jamie.Holcombe@uspto.gov Signature: Users, Holcombe, Henry Digitally signed by Users, Holcombe, Henry Date: 2023.03.16 16:29:18 -04'00' Date signed: ______________________________
Co-Authorizing Official Name: Frederick Steckler Office: Office of the Chief Administrative Officer (OCAO) Phone: (571) 272-9600 Email: Frederick.Steckler@uspto.gov Signature: Users, Steckler, Frederick W. Digitally signed by Users, Steckler, Frederick W. Date: 2023.04.12 18:30:50 -04'00' Date signed: ______________________________	