Version Number: 09-2016

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

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

U.S. Department of Commerce Privacy Threshold Analysis

USPTO Corporate Administrative Office System (CAOS)

Unique Project Identifier: PTOC-005-000

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 Senior Agency Official for Privacy (SAOP).

Description of the information system and its purpose:

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

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

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

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

WebTA provides the following functionality:

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

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

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

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

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

Questionnaire:

1. 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. *Continue to answer questions, and complete certification.*

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

☒ 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 about: *(Check all that apply.)*

☐ Companies

☐ Other business entities

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

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

☒ Yes, WebTA and COOP-WB collects, processes, maintains, and disseminates/transmits information in identifiable form from or about USPTO employees and supporting contractors.

☒ DOC employees

☒ Contractors working on behalf of DOC

☐ 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 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.

4c. 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, and/or 4c are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

☒ I certify the criteria implied by one or more of the questions above **apply** to the Corporate Administrative Office System and as a consequence of this applicability, I will perform and document a PIA for this IT system.

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

Name of System Owner (SO): Colleen Sheehan

Signature of SO: Users, Sheehan, Colleen Digitally signed by Users, Sheehan, Colleen DN: dc=gov, dc=uspto, cn=Users, cn=Sheehan, Colleen Date: 2017.08.01 18:03:51 -04'00' Date: 08/01/2017

Name of Senior Information Security Officer (SISO): Rami Dillon

Signature of SISO: [signature] Date: 8/2/17

Name of Co-Authorizing Official (AO): Frederick Steckler

Signature of AO: [signature] Date: 8/2/2017

Name of Co-Authorizing Official (AO): John B. Owens II

Signature of AO: [signature] Date: 8/3/17

Name of Bureau Chief Privacy Officer (BCPO): John B. Owens II

Signature of BCPO: [signature] Date: 8/3/17