U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Corporate Administrative Office System

PTOC-005-000

September 4, 2015

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

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:

- 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.
- 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) Office of Human Resources (OHR) Human Resources Division's (HRD) 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) Workbooks 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 Workbook/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.

Sustainable Planner 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 information is collected (e.g., nature and source)?

   WebTA contains and collects USPTO employee Social Security numbers to process payroll transactions, personal leave balances; time and attendance awards information, employee relations information, labor relations information, position description and management information.

   For COOP, Individual COOP officers in the various major Offices and Business Units within USPTO will supply information and requirements supporting emergency Continuity of Operations for the USPTO, containing the following for each offices/unit:

   - Primary processes
   - Business impacts
   - Necessary staff/employee resources (names, personal home number, personal cell number, personal email) – and loss of employee strategies and line of succession
   - Office resources (number, space, specialized capabilities, occupancy, etc) – strategies/tasks for mitigate loss
   - Hardware (computers, hardware, phones, specialized and/or shared equipment, etc) – strategies/tasks for mitigate loss
   - Software resources (applications, versions, vendors, etc) – strategies/tasks for mitigate loss
   - Critical IT applications – strategies/tasks for mitigate loss
   - Communications services/methods/strategies – strategies/tasks for mitigate loss
   - Intra-agency/extra-agency dependencies/workflows
   - Regulatory reporting requirements
   - Emergency operating records

2. Why is this information being collected (e.g., to determine eligibility)?

   WebTA captures employee Social Security numbers in order to collect, verify, and electronically certify time and attendance information. This information is further collected for transmission over the USPTO network to the National Finance Center (NFC).

   COOP information is collected in database-like fields (entered by the Business Unit COOP staff) and populates a database record for each business unit/office. With that information, per office, the COOP Managers can run reports to track the required staff, office space, hardware, software, phones, printers, etc necessary to maintain operational continuity/capacity for USPTO and/or specific offices therein in times of some unforeseen emergency event (fire, flood, inclement weather, closed facilities, etc) up to and including re-positioning/assigning that staff to an alternate location/site for limited/extended durations.

3. What is the intended use of information (e.g., to verify existing data)?

This information is used by the CAOS WebTA, which captures employee Social Security numbers in order to collect, verify, and electronically certify time and attendance information. This information is further collected for transmission over the USPTO network to the National Finance Center (NFC).

The COOP information is to be used only in reporting to the COOP Manager and USPTO Senior Management, creation of the overall USPTO COOP Workbook.

4. With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?

   WebTA:
   The information is shared with the National Finance Center (NFC).

   COOP:
   The information will be shared internally to the COOP Office and with USPTO Senior Management (via reports and the overall Workbook).

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how can individuals grant consent?

   WebTA:
   Employee PII information (Social Security Numbers) initially collected during employment application process is further used by and contained within WebTA to process payroll, time and attendance, and leave balances data.

   COOP:
   The information required to populate the COOP Workbook is not personal in nature. Other than the personal/home phone numbers and personal emails for each of the designated COOP necessary staff, there is no personal information. In the cases of those selected as "necessary staff," the phone numbers and emails are subject to their personal scrutiny, but their refusal to include it would probably negate them being in the pool of necessary staff selected.

6. How will the information be secured (e.g., administrative and technological controls)?

   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 1 *Guide for Assessing the Security 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.
2. The USPTO Personally Identifable Data Extracts Policy.

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. Aditional operation controls include: (1) Logical edit checks to ensure proper sequence of actions; (2) Physical terminal identification; (3) Database UserID; (4) Restricted data display, as required; and (5) Restricted access.
2. Manual procedures shall be followed for handling extracted data containing sensitive PII, which is physically transported outside of the USPTO premises. In order to remove data extracts containing sensitive PII from USPTO premises, users must:
    a. Maintain a centralized office log for extracted datasets that contain sensitive PII. This log must include the date the data was extracted and removed from the facilities, a description of the data extracted, the purpose of the extract, the expected date of disposal or return, and the actual date of return or deletion.
    b. Ensure that any extract which is no longer needed is returned to USPTO premises or securely erased, and that this activity is recorded on the log.
    c. Obtain management concurrence in the log, if an extract aged over 90 days is still required.
    d. Store all PII data extracts maintained on an USPTO laptop in the encrypted My Documents directory. This includes any sensitive PII data extracts downloaded via the USPTO Virtual Private Network (VPN).
    e. Encrypt and password-protect all sensitive PII data extracts maintained on a portable storage device (such as CD, memory key, flash drive, etc.). Exceptions due to technical limitations must have the approval of the Office Director and alternative protective measures must be in place prior to removal from USPTO premises.

7. How will the data extract log and verify requirement be met?

USPTO has not developed a centralized logging system for PII data extracts. Such a system would track the following categories of information:

- Who performed the extract
- When extract was done
- What was the extract
- Where was the extract taken from
- Has the extract been deleted
- If not deleted after 90 days, to monitor that it is still needed in 90 day intervals.

Until a system is implemented, USPTO is using the following compensating controls to protect II data:

- No extracts of sensitive data may be copied on to portable media without a waiver approved by DOC CIO. The request for a waiver must include specifics as to how the data and device are protected, how long the data will be maintained, and how the data on the device will be deleted when no longer required.
- All laptop computers allowed to store sensitive data must have a full disk encryption in place.
- All remove access to public USPTO systems containing sensitive data must be encrypted. All remote access to internal USPTO systems containing sensitive data must fully comply with DOC Remote Access Policy requirements.
- All flexiplace/telework agreements for working off site require that adequate data protection be in place.

8. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

   The existing system of records covers the information residing in the database. These include: COMMERCE/DEPT-18, Employee Personnel Files Not Covered by Notices of Other Agencies.

   For COOP, the Continuity of Operations records information is being created and covered. http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/records_mgmt_crs.html

   Under Office of the Chief Administrative Officer: http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/docs/OCAO.pdf , GRS 3.2:10.

9. Are these records covered by a record control schedule approved by the National Archives and Records Administration (NARA)?

   GRC 20 allows agency determination that certain electronic records are authorized for erasure of deletion when they are no longer needed for administrative, legal, audit, or other operational purposes.

   Electronic records that represent hard copy records can be deleted after expiration of the retention period authorized for the hard copy records.

   For COOP, the Continuity of Operations records information is being created and covered. http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/records_mgmt_crs.html

Under Office of the Chief Administrative Officer:
http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/docs/OCAO.pdf , GRS 3.2:10.

SIGNATORY AUTHORITY

Agreed: _____ 9/17/2015

Colleen Sheehan — Date

Information System Owner

Agreed: _____ 9/17/2015

John Pardun — Date

Senior Information Security Officer

Agreed: _____ 9/24/2015

Frederick Steckler — Date

Co-Authorizing Official

Agreed: _____ 9/22/15

John B. Owens II — Date

Co-Authorizing Official