U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Corporate Administrative Office System (CAOS)

PTOC-004-00

July 22, 2011

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 a Major Application (MA). 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:

- Provide USPTO management and employees the capability to manage, review and receive training necessary to become fully competent in their jobs.
- 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.

The CAOS consists of the following five (3) AISs:

The Office of Human Resources National Finance Center System (OHRS) implements the following National Finance Center (NFC) developed HR systems within the United States Patent and Trademark Office (USPTO):

- **Entry Processing, Inquiry, and Correction System (EPIC)** allows OHR staff to enter payroll and personnel transactions for processing in the NFC payroll/personnel system.

- **Statement of Earnings and Leave (EARN)** allows OHR staff to view and print employee's Statements of Earnings and Leave.

- **Special Payroll Processing System (SPPS)** allows OHR staff to process quick service payments, final salary payments for indebted employees, and payments to the estate of a deceased.

- **W-2 System (WTWO)** allows OHR staff to view and print an employee's W-2, Wage and Tax Statement data.

OHRS primary users include staff of Office of Human Resources inside the PTO firewall.

The Time and Attendance Automated System (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 users include USPTO employees, managers, and administrators. WebTa provides the following functionalities:

- 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

Emergency Notification System (ENS)

- AtHoc Notifications Server – provides central application functionality, as well as web based administration and alert activation console.
- AtHoc Publisher, including Alerts Publisher and Manager – web based application to publish and manage alerts, including pre-defined alerts, based on alert type and publisher's rights and permissions.
- Web based administration console - allowing for central system administration using a role and permissions based secure access model.
- Desktop Alerts Software – small footprint standard based software client installed on end-user desktops, deployed via Microsoft System Management Server (SMS) or other remote installation applications. The desktop software is responsible for the timely communication with the AtHoc Notification Server via HTTP or HTTPS to receive alerts and display the desktop popup visual and audio cues.

Alert Targeting Server Module – a module running on the Notifications Server, enabling publishers to target alerts to specific groups of users based on groups defined in the base's user directory (i.e. LDAP or Active Directory). Integration with LDAP or Active Directory is required to enable use of this module.

QUESTIONNAIRE

1. What information is collected (e.g., nature and source)?

   CAOS (OHRS) contains and collects USPTO employee's social security numbers to process payroll transactions, personal leave balances; time and attendance (WebTA) awards information, employee relations information, labor relations information, position description and management information.

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

   WebTA captures employee's 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).

   OHRS contains employee's PII information to process payroll and personnel transactions, quick service payments, final salary payments for indebted employees, and payments to the estate of a deceased; view and print an employee's W-2, Wage and Tax Statement data, and employee's statements of Earning and Leave.

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

   The intended use of information is to support CAOS role and mission.

   The information is used to perform initial evaluations of the fitness of applicants for employment at the USPTO and for supporting the decision-making activities of managers and analysts in the USPTO business areas. This information is further used by the CAOS WebTA which captures employee's 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).

   OHRS contains employee's PII information to process payroll and personnel transactions, quick service payments, final salary payments for indebted employees, and payments to the estate of a deceased; view and print an employee's W-2, Wage and Tax Statement data, and employee's statements of Earning and Leave.

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

   OHRS and WebTA:

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

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?

   Applicants must submit essential information to ensure that their qualifications for employment can be examined and verified during initial employment application. Applicants can always refuse to provide information, but their applications will not be screened further. Submission functions as consent for use of the information for the intended purpose.

Employee's PII information (social security numbers) initially collected during employment application process is further used by and contained within OHRS and WebTA systems to process payroll, time and attendance, and leave balances data.

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. 2, 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, Continuous Monitoring reviews, and triennial assessments 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 2, *Recommended Security Controls for Federal Information Systems* and NIST SP 800-53A Final *Guide for Assessing the Security Controls in Federal Information Systems*. 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 Plans specifically address 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 Identifiable 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. Additional 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.

Encrypt and password-protect prior to transmission any sensitive PII data extracts that are sent to an external e-mail address via the Internet. The password key should be forwarded to the recipient in a separate e-mail from the attached file.

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 PII 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
   - All remote 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?

   No, there is no new system of records being created. 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.

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

   No. 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.

SIGNATORY AUTHORITY

Agreed: _____ _____/_____/_____

Colleen Sheehan Date

Information System Owner