U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Background Investigation and Tracking System

PTOC-009-00

September 15, 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 USPTO Background Investigation and Tracking system (BITS) suite of Web-based applications is currently hosted under a contract within Equinix Data Center in Ashburn, VA, 20164. MicroPact provides a fully managed support infrastructure service including: supporting hardware and software, secure computing facilities, Internet gateway communications security, system administration, and system and application security services.

The purpose of this project is to deploy a web enabled system in support of the USPTO requirement to migrate from a FoxPro based system to a more robust, flexible and enterprise capable background investigation tracking system. The goal is to deploy a system that is able to represent the evolving business processes of USPTO and incrementally introduce additional departments into the user population.

Users access the USPTO BITS system via the Internet with the additional requirement of being logged onto the USPTO network and accessing BITS via the USPTO INTRANET. All of the logic and processing functionality of USPTO BITS resides on one or more central servers, with users accessing USPTO BITS from their PC client Web browsers.

QUESTIONNAIRE

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

   The Micropact USPTO BITS system collects following personal identifiable information including: individual names, date of birth, place of birth, phone number and social security numbers for background investigation tracking.

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

   The information is collected to track the proper background investigations on the possible USPTO employment candidates and to conduct reinvestigations as needed. The information is collected in order to show whether candidates are reliable, trustworthy, of good character and loyal to the United States.

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

   The information is collected to track the status of the background investigations (which are required to determine a candidate's eligibility for employment and/or access to national security information).

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

   The information will primarily stay within the USPTO Office of Security and Safety and is shared with properly credentialed background investigators who are conducting the background investigation and employees from the Office of Human Resources, Employee Relations Division who conduct suitability adjudication on USPTO employees.   It will also be shared with other federal agency security offices that require the 'passing' of USPTO background investigative data for USPTO personnel visiting/attending meetings/conferences/briefings at other federal agencies.

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?

   All information requested is provided on a voluntary basis. USPTO as part of the U.S Government is authorized to ask for this information under Executive Orders 10450 and 10577. Social Security Number (SSN) is needed in order to keep records accurate, because other people may have the same name and birth date. The executive Order 9397 also asks Federal Agencies to use SSN to help identify individuals in agency records. As such the information is required in order to conduct adequate background investigation to be considered for employment with the USPTO.

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

The information is secured in accordance with the NIST 800-53, Revision 4 security controls. Secured technical architecture is incorporated into the system to prevent any unauthorized access to the personally identifiable data. Data is maintained in areas accessible only to authorized personnel and systems are password protected.

Management Controls:

1. The Micropact USPTO BITS follows the USPTO SDLC review process to ensure that management controls are in place for the system. During the enhancement of any component, the security controls are reviewed, re-evaluated, and updated in the System Security Plan (SSP). The SSP 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 check on all personnel, including contractor staff.

2. The USPTO IT Privacy Policy and Personally Identifiable Data Extracts Policy are followed and implemented.

Operational Controls:

1. Automated operational controls include securing all hardware associated with BITS in the Micropact Data Center. The Data Center is controlled by access card entry and all use of the card is audited through the access system to restrict access to the servers, their Operating Systems and databases. In addition, physical access points to the Micropact Data Center is controlled by physical locking mechanism including separate door locks, an alarm control contact monitored twenty-four (24) hours a day by ADT, a motion detector at each door and hallway and a video camera at each hallway.

   Contingency planning has been prepared for the data. Backups are performed on the processing databases. All backup tapes that contain PII or information covered under the Privacy Act are encrypted with FIPS 140-2 compliant algorithms by the MicroPact Database Administration Team.

Technical controls:

1. Information is also secured through the application itself, by only allowing authorized users access to the application and to data to which they have access and privilege. Also the information system controls attacks and unauthorized attempts on the application and database through strict logins, AV protection, and through firewalls.

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

   The Micropact USPTO BITS system includes databases that store PII data related to USPTO background investigations. As a result, Micropact has implemented security controls to meet the data extract log and verify requirements identified in OMB M-07-16. Refer to the Audit and Accountability Controls (AU) in the latest Micropact USPTO BITS SSP for specific implementation details.

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

   The system of records is planned to be created under the Privacy Act, 5 U.S.C 522a and is identified as "Investigative and Security Records—Commerce/Dept-13".These files will be available at the following URL: *http://www.gpo.gov/fdsys/pkg/PAI-2005-COMMERCE/html/PAI-2005-COMMERCE-SYSTEMOFRECORDS-COMMERCE-DEPT-13.htm*

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

   Background Investigation and Tracking files that contain PII information are covered by the USPTO Comprehensive Records Schedule approved by NARA as detailed at the following URL: *http://ptoweb.uspto.gov/ptointranet/cisd/cio/records_mgmt/records_mgmt_crs.html*, under the Office of Chief Administrative Officer records. Additional record control schedule information is available on NARA's website: *http://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-commerce/rg-0241*.

SIGNATORY AUTHORITY

Agreed: ______________________________ 9 / 17 / 15

Joseph Burns — Date

Information System Owner

Agreed: ______________________________ 9 / 21 / 15

John Pardun — Date

Senior Information Security Officer

Agreed: ______________________________ 9 / 22 / 15

John B. Owens II — Date

Co - Authorizing Official

Agreed: ______________________________ 9 / 24 / 15

Frederick Steckler — Date

Co - Authorizing Official