



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

IT PRIVACY POLICY OCIO-6008-09

Date of Issuance: May 22, 2009
Effective Date: May 22, 2009
Review Date:

TABLE OF CONTENTS

Section

- I. PURPOSE
- II. AUTHORITY
- III. SCOPE
- IV. DEFINITIONS
- V. POLICY
- VI. RESPONSIBILITIES
- VII. EFFECT ON OTHER POLICIES

I. PURPOSE

This policy establishes the uniform policy within USPTO for IT Privacy of Personally Identifiable Information (PII) which is processed, stored, or transmitted on USPTO automated information systems (AISs) and within and across the USPTO IT infrastructure. The Department of Commerce has identified four principles necessary to protect Personally Identifiable Information (PII):

- **Data Minimization:** The United States Patent and Trademark Office shall collect the minimal amount of information necessary from individuals consistent with the Office's mission and legal requirements.
- **Transparency:** Notice covering the purpose of the collection and use of PII shall be provided in a clear manner. All PII collected shall not be used for any other purpose unless authorized or mandated by law.
- **Accuracy:** Any PII collected shall be maintained in a sufficiently accurate, timely, and complete manner to ensure that the interests of the individuals are protected.
- **Security:** Adequate physical and IT security measures shall be implemented to ensure that the collection, use, and maintenance of PII is properly safeguarded and the information is both authorized for release to the public as appropriate as well as promptly destroyed in accordance with approved records control schedules. The management principles in this policy apply to all USPTO systems and represent minimum standards and configurations to be used by all USPTO employees and contractor employees.

IT PRIVACY POLICY

USPTO's Agency Administrative Order (AAO) 212-4 and the USPTO IT Security Handbook state that all USPTO information, applications, systems, networks, and IT infrastructure and resources must be protected from loss, misuse, and unauthorized modification, disclosure, or access. The intent of this document is to establish a policy for securing PII stored on all USPTO computer systems within USPTO and contractor facilities, with the exceptions noted below.

II. AUTHORITY

This policy is issued pursuant to:

- The Federal Information Management Security Act of 2002 (FISMA)
- USPTO IT Security Policy Management Policy

III. SCOPE

The provisions of this policy apply to all USPTO employees and contractor employees using or operating USPTO AISs and to contractor employees providing services to the USPTO who use USPTO AISs and networks. This policy applies to all USPTO AIS or resources, independent of size. For example, it applies to desktops, laptops, personal data assistants (PDAs), servers, and network devices to include firewalls, intrusion detection systems, intrusion prevention systems, routers and switches. Additionally, this policy applies to all types of media used to record USPTO data which includes, but is not limited to: hard drives, CDs, DVDs, other magnetic media such as floppy disks, and solid-state media (flash memory, memory stick, USB flash drive, etc.).

This policy also applies to those AIS operated and used by contractor employees, guest researchers and collaborators to carry out the USPTO mission, whether or not they are owned, leased, or on Government property. This policy must be explicitly addressed in all IT procurement activities.

All provisions of this policy shall be fully implemented within 180 calendar days of its issuance.

IV. DEFINITIONS

Adequate Security: Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to, or modification of, information.

Automated Information System (AIS): A combination of functional users, information technology personnel, business processes and procedures, application software, system software, documentation, commercial off-the-shelf software (COTS), computers, networking and other information technology resources that collect, record, process, store, retrieve, display, and disseminate information and data.

Personally Identifiable Information (PII). USPTO identifies two kinds of PII:

- Protected PII: Information that can be used to (i) uniquely identify (e.g., date of birth, gender, race, social security number, credit card account number, photograph, medical information, education information, etc.); (ii) contact (e.g., home address, personal phone number, etc.), or (iii) locate an individual (e.g., home address, etc.).

IT PRIVACY POLICY

- **Publicly Releasable PII:** Information identifiable to a specific individual that has been authorized for public release. The following information is publicly releasable PII: Non-financial information regarding business entities, such as business addresses, telephone numbers, web sites, e-mail as well as information available on the USPTO public website such as employee name, identification number, phone number and office location.

Privacy Impact Assessment (PIA): An analysis of how information is handled to: (i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and, (iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Threshold Analysis (PTA): An analysis designed to help identify whether privacy information will exist on a planned system as well as to determine whether a PIA is needed.

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features (e.g., role-based access), management constraints, personnel security, and security of physical structures, areas, and devices (Synonymous with security controls and countermeasures).

V. **POLICY**

In order to effectively maintain and protect PII information, all USPTO employees and contractor employees are responsible for proper use of all PII residing on any AIS(s) that they possess or access. All USPTO employees and contractor employees must follow the mandatory practices within this policy in the creation and management of PII.

In order to protect PII, it is imperative that all USPTO employees and contractor employees adhere to the following guidelines:

- All USPTO employees and contractor employees are prohibited from transferring and storing any USPTO protectable PII to personally owned equipment by any means, including: data entry, any type of removable media, LAN/WAN telecommunications, VPN, or, wireless telecommunications.
- All external and removable devices and digital/recording media, including, but not limited to, flash memory/memory cards, PDAs, hard drives, CDs, DVDs, and floppy disks, are prohibited from being used to store protectable PII unless approved in advance via an Enterprise Asset Management System (EAMS) change record by the CIO. Official data backups that require such media are exempt from this requirement.
- All protectable PII information is prohibited from being removed from the USPTO physical perimeter (this perimeter includes satellite offices) unless it resides on a FIPS 140-2 compliant encrypted device. The only exceptions are: (i) back-up media transported to an approved off-site location, and (ii) specific requests for removal previously authorized in writing by the USPTO CIO.
- All laptops that contain or may contain protectable PII must have full-disk encryption in accordance with FIPS 140-2 compliant algorithms. Any laptop incapable of providing FIPS 140-2 compliant encrypting protection services is prohibited from storing PII under any circumstances.

IT PRIVACY POLICY

- Remote access to USPTO systems that contain protectable PII is allowed only with two-factor authentication where one of the factors is provided by a device separate from the computer requesting access. For the purposes of this policy, web mail solutions are excluded from this requirement.
- For remote access to and mobile devices that access USPTO systems with PII, a time-out function must be configured requiring user re-authentication after 30 minutes of inactivity.
- All USPTO systems that store protectable PII shall have sufficient auditing enabled, in accordance with OMB M-06-16, to effectively investigate the compromise or potential compromise of data.
- Disposal of PII from systems shall be done in a manner that complies with the approved records retention schedule for those records.
- Reduce the volume of collected and maintained PII information to the minimum necessary for IT system functionality and business requirements.
- As part of the USPTO System Development Life Cycle process (SDLC), a Privacy Threshold Analysis (PTA) shall be conducted prior to the development or procuring of any IT system or for significant modification to an IT system. A Privacy Impact Assessment (PIA) shall be conducted if the results of the PTA indicate privacy information is present. The information captured during the PIA includes:
 - Types of information that will be collected (nature and source);
 - Why the information needs to be collected;
 - Intended use of the information;
 - With whom the information will be shared;
 - What opportunities individuals have to decline or consent to providing information, and how individuals can consent;
 - How the information will be secured; and
 - Whether a system of records is being created under the Privacy Act.

All USPTO employees and contractor employees shall immediately report actual or suspected incidents involving the compromise of PII as soon as they occur to their supervisor(s) or other appropriate supervisory channels, and promptly call or e-mail the USPTO Help Desk. Refer to the USPTO Breach Notification Policy for additional policies on reporting requirements.

VI. RESPONSIBILITIES

All USPTO employees and contractor employees shall adhere to this policy and shall not engage in any activity that might circumvent its provisions. All USPTO employees or contractor employees responsible for the management, implementation, installation, configuration, operation, maintenance, or security of a USPTO AIS or network must implement the mandatory practices of this policy and must identify any proposed deviations from the mandatory practices of this policy and request a waiver in writing from the

IT PRIVACY POLICY

USPTO Policy, Privacy, and PKI Division (PPPD) in accordance with the waiver process as defined in the USPTO IT Security Handbook.

The IT Security Management Group (ITSMG) shall be responsible for monitoring user compliance with this policy as part of the periodic IT security self-assessment program or automated AIS evaluations and maintaining current, approved waivers as part of the documentation for appropriate system security plan(s). The PPPD is responsible for maintaining and updating this policy; reviewing, approving or denying waivers; and, monitoring compliance through bi-annual compliance reviews.

System owners shall implement the mandatory practices of this policy for each USPTO AIS for which they are responsible, unless a system is covered by a current, approved waiver. *USPTO's AAO 212-4, Section III, IT Security Roles and Responsibilities*, identifies key USPTO roles that have both IT Security and C&A responsibilities.

Compliance with this policy shall be enforced through oversight, inspection, administrative, disciplinary, and corrective actions. As part of this policy, a USPTO Senior Privacy Official must be designated to oversee all issues specific to privacy information and compliance.

The USPTO Help Desk (HDS) shall create incident records upon being informed of a suspected loss or compromise of privacy information. The USPTO Help Desk shall inform the Office of Corporate Services upon notification of loss or theft of IT systems suspected of housing privacy information. The USPTO Help Desk shall also inform the USPTO Computer Incident Response Team (CIRT) upon notification of suspected compromise of privacy information.

The Administrative Management Group (AMG) shall be responsible for ensuring IT procurement contracts explicitly refer to this policy and that contractors are in compliance.

All incidents involving loss or compromise of PII shall be reported by the USPTO CIRT to the DOC IT CERT, who in turn informs the US-CERT within one hour of discovering the incident. Please refer to the *U.S. Department of Commerce, IT Security Program Policy and Minimum Implementation Standards* for additional process guidance, and the upcoming Breach Notification Policy.

VII. EXCEPTIONS

Please refer to the waiver process as defined in the USPTO IT Security Handbook.

VIII. REFERENCES

- *E-Government Act (Public Law 107-347), Title III - Federal Information Security Management Act (FISMA)*, December 2002.
- *Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules*, February 2004.
- *FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- *FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

IT PRIVACY POLICY

- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, Revised November 2000.
- OMB Memorandum M-03-22 *Guidance for implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB M-06-15, *Safeguarding Personally Identifiable Information*, May 2006.
- OMB M-06-16, *Protection of Sensitive Agency Information*, June 2006.
- OMB M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007
- The Privacy Act of 1974, 5 U.S.C. §552a
- U.S. Department of Commerce, *IT Privacy Policy*.
- U.S. Department of Commerce, *IT Security Program Policy and Minimum Implementation Standards*, June 30, 2005.
- U.S. Patent and Trademark Office, *Agency Administrative Order 212-4, USPTO IT Security Handbook*.
- U.S. Patent and Trademark Office, *IT Privacy Policy*.
- U.S. Patent and Trademark Office, *Rules of the Road*.
- U.S. Patent and Trademark Office, *Comprehensive Records Schedule*.

IX. EFFECT ON OTHER POLICIES

This policy affects all new, revised, or retired policies issued in Fiscal Year 2009.

ISSUED BY:



John B. Owens II
Chief Information Officer
United States Patent and Trademark Office

OFFICE OF PRIMARY INTEREST: IT Security Management Group