



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

BREACH NOTIFICATION POLICY OCIO-6007-09

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. EXCEPTIONS
- VIII. EFFECT ON OTHER POLICIES

I. PURPOSE

This policy establishes the uniform policy within the United States Patent and Trademark Office (USPTO) for reporting breaches specific to Personally Identifiable Information (PII) processed, stored, or transmitted on USPTO computer systems and within and across the USPTO Information Technology (IT) infrastructure.

The Privacy Act of 1974 (Pub. L. No. 93-579) requires each federal agency to:

- **Establish Rules of Conduct:** Agencies are required to establish “rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance.” (5 U.S.C. § 552a(e)(9)).
- **Establish Safeguards:** Agencies are also required to “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.”
- **Maintain accurate, relevant, timely and complete information:** The Privacy Act requires PII within a system of records to be maintained in a manner that is accurate, relevant, timely, and complete.

BREACH NOTIFICATION POLICY

It is important for agencies to fulfill their responsibilities with respect to identifying systems of records and developing and publishing notices as required by the Privacy Act and the Office of Management and Budget's (OMB's) implementing policies. By collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it.

USPTO's IT Security Handbook, states 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 reporting unauthorized disclosure of personally identifiable information (PII), stored on all USPTO computer systems within USPTO and contractor facilities.

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, accessing or using USPTO data, and to contractor employees providing services to the USPTO who use USPTO Automated Information Systems (AISs), data and networks. It applies to all USPTO AISs or resources, independent of size. Additionally, this policy applies to all types of media used to store USPTO PII which include, but are not limited to: hard drives, CDs, DVDs, other magnetic media such as floppy disks, and solid-state media (flash memory, memory stick, Universal Serial Bus (USB) flash drive, thumb drive etc.). Finally, it applies to all media output (soft and hard-copy) that contain USPTO PII.

This policy also applies to AISs and equipment, including network devices, operated and used by contractor employees, guest researchers, collaborators, and other federal agencies to carry out the USPTO mission, whether or not they are owned, leased, or on government property. It shall be explicitly addressed in all IT procurement activities.

This policy pertains to both electronic, hard-copy (paper) records and microfilm.

All provisions of this policy shall be fully implemented within 90 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.

BREACH NOTIFICATION POLICY

Breach: The terms “breach” and/or “incident” as used in this document include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording.

Personally Identifiable Information - USPTO identifies two kinds of PII:

- Protected PII: Information that can be used to uniquely identify (e.g., date of birth, gender, race, social security number, credit card account number, medical information, education information, etc.) contact (e.g., home address, home phone number, etc.) or locate an individual (e.g., home address)
- 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 addresses
 - Information available on the USPTO public website such as employee name, work phone number and office location

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

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).

System of Records: A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

V. POLICY

To effectively safeguard and report breaches specific to PII, all USPTO employees and contractor employees are responsible for proper handling of PII in either hard-copy format or on any computer systems that they possess, or to which they have management responsibility. All USPTO employees and contractor employees must follow the mandatory practices within this policy with respect to safeguarding and reporting unauthorized disclosure specific to PII.

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

BREACH NOTIFICATION POLICY

Incident Reporting and Handling

- All USPTO employees and contractor employees shall be responsible for reporting physical and logical IT security violations involving PII that they are aware of to their supervisor(s) or other appropriate supervisory channels and promptly call or e-mail the USPTO Help Desk Services Division (HDSD).
- All USPTO employees and contractor employees shall be responsible for reporting to their supervisor(s) or other appropriate supervisory channels clear weaknesses that potentially put PII at risk.
- The HDSD shall create incident records upon being informed of a suspected loss or unauthorized disclosure of PII.
- The HDSD shall inform the Office of Corporate Services upon notification of loss or theft of IT systems or devices suspected of housing PII.
- The HDSD shall also report all incidents related to the unauthorized disclosure of PII, including PII in paper format and loss or theft of IT systems or devices suspected of housing PII, to the USPTO Computer Incident Response Team (CIRT) by email at CIRT@USPTO.GOV.
- The USPTO CIRT shall use a set of formal mechanisms and procedures¹ to ensure quick, consistent, and decisive action when an incident occurs.
- Unauthorized access or any incident involving PII is to be reported by the USPTO CIRT to the US-CERT and the DOC CIRT within one hour of discovery/detection. Reportable incidents include:
 - When an individual gains logical or physical access without permission to a Federal agency network, system, application, data, or other resource.
 - When there is a suspected or confirmed breach of PII regardless of the manner in which it might have occurred.
- The USPTO CIRT shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication of vulnerability, recovery, and monitoring.
- The USPTO CIRT shall prepare a final report, with USPTO ITSO concurrence, following the completion of all incident response activities. Furthermore, the affected system(s) shall be declared operational.

With a PII loss or breach reported, an internal investigation shall be conducted to assess the circumstances surrounding the loss, enabled counter-measures in place at time of the loss, and also includes other variables.

¹ Refer to the *USPTO IT Security Handbook* for incident severity levels and courses of action.

BREACH NOTIFICATION POLICY

Refer to *USPTO's AAO 212-4*, *USPTO IT Security Handbook* and *U.S. Department of Commerce, IT Security Program Policy and Minimum Implementation Standards* for additional Incident Reporting and Handling policies and processes.

NOTE: IT security incident report information shall be treated as sensitive information and safeguarded appropriately. Access to IT security incident information shall be restricted and stored in a secured area.

External Breach Notification

The Department of Commerce shall, on the behalf of USPTO, notify external sources of IT security breaches based on evaluation of specific elements necessary for the USPTO to determine the scope of the breach and, if applicable, help restore the reasonable integrity of the compromised system.

VI. RESPONSIBILITIES

All USPTO employees and contractors shall adhere to this policy and shall not engage in any activity that might circumvent its provisions. Such activities include, but are not limited to;

- Failing to implement and maintain security controls, for which an employee is responsible and aware, for PII regardless of whether such action results in the loss of control or unauthorized disclosure of PII
- Exceeding authorized access to, or disclosure to unauthorized persons of, PII
- Failing to report any known or suspected loss of control or unauthorized disclosure of PII

All USPTO employees or contractor employees responsible for the management, implementation, installation, configuration, operation, maintenance, or security of a USPTO AIS must implement the mandatory practices of this policy and must identify any proposed deviations from the mandatory practices of this policy by requesting a waiver in writing from the USPTO IT Policy, Privacy, and PKI Division (PPPD) in accordance with the waiver process as defined in the *USPTO IT Security Handbook*.

The Administrative Management Group (AMG) is responsible for ensuring this policy is referenced in all contractor IT procurement activities and for monitoring contractor compliance with this policy.

The IT Security and Management Group (ITSMG) shall be responsible for the monitoring of user compliance with this policy as part of the periodic IT security self-assessment program or AIS evaluations, and shall maintain 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 the conduct of 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*, *USPTO IT Security Handbook*, identifies key system owner responsibilities.

BREACH NOTIFICATION POLICY

The Department of Commerce has created an Identity Theft Task Force, whose mission is to provide advance planning, guidance, in-depth analysis, and a recommended course of action in response to a data breach. The permanent core members are:

- Chief Information Officer - Chair
- Chief Financial Officer - Voting Member
- Office of the General Counsel - Voting Member
- Office of Legislative and Intergovernmental Affairs - Voting Member
- Office of Public Affairs - Voting Member
- Chief of Staff - Voting Member
- Senior Policy Advisor - Voting Member
- Office of the Inspector General - Non-Voting Member

The Office of the Chief Information Officer (OCIO) shall ensure routine briefings occur so that circumstances surrounding a particular PII disclosure incident can be discussed, which include cross-departmental trends and analysis of PII and related losses. Additionally, the OCIO must ensure that a senior representative be made available during any ID Theft Task Force meeting to discuss any program or policy issues that are relevant to the breach or incident.

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 shall be designated to oversee all issues specific to privacy information and compliance.

VII. EXCEPTIONS

Exceptions to this policy shall be determined on a case-by-case basis using the by using 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.
- 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*

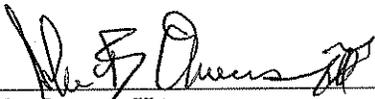
BREACH NOTIFICATION POLICY

- 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