



## UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

### NETWORK AND AIS AUDIT, LOGGING, AND MONITORING POLICY OCIO-6011-09

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

#### TABLE OF CONTENTS

#### Section

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

#### **I. PURPOSE**

This policy establishes the uniform policy within the United States Patent and Trademark Office (USPTO) for the auditing, logging, measurement, and monitoring of networks and automated information systems (AIS). This policy establishes minimum practices to ensure USPTO systems and networks are audited to maintain awareness of the operating environment, to detect indications of security problems, and to ensure USPTO AIS systems and networks are used for authorized purposes.

#### **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 computer systems, as well as the systems and networks, and to contractor employees providing services to the USPTO by using USPTO AIS and networks. This policy applies to production AIS, servers and server applications only.

## **IV. POLICY**

### **A. General Policy**

It is USPTO policy that audit trails shall be used for the following:

1. **Individual Accountability.** Audit trails shall be used to support accountability by providing a trace of user actions.
2. **Reconstruction of Events.** Audit trails shall be used to support after-the fact investigations of how, when, and why normal operations ceased.
3. **Intrusion Detection.** Audit trails shall be designed and implemented to record appropriate information to assist in intrusion detection.
4. **Problem Identification.** Audit trails shall be used as online tools to help identify problems other than intrusions as they occur.

All USPTO operational information technology (IT) systems shall enable audit and normal logging processes within the scope previously defined.

### **B. Contents of Audit Trail Records**

An audit trail shall include sufficient information to establish what activity occurred and who (or what) caused them. Given the diversity of IT systems' capabilities and missions, the scope and contents of the audit trail shall balance security needs with performance needs, privacy, and costs.

The following list is representative of events that would provide an acceptable audit trail and is included in this policy as guidance.

- User login – unsuccessful, successful if feasible
- Server startup and shutdown
- Service startup and shutdown -- unsuccessful and successful, if feasible
- User account permission modifications -- unsuccessful and successful
- User account additions and deletions -- unsuccessful and successful
- IP address or hostname associated with a given event, if feasible
- Firewall rule base modification, if applicable -- unsuccessful and successful
- Software installation or removal -- unsuccessful and successful, if feasible

Audited events shall be documented in the appropriate system security plan or baseline configuration document of that operating system, network device, or application.

### **C. Audit Trail Security**

Audit trails shall be protected from unauthorized access. The following precautions shall be taken:

- Control online audit logs. Access to online audit logs shall be strictly controlled.

## NETWORK AND AIS AUDIT, LOGGING, AND MONITORING POLICY

- Separation of duties. Separation of duties between security personnel who administer the access control function and those who administer the audit trail shall be ensured.
- Protect confidentiality. Confidentiality of audit trail information shall be ensured.
- Audit logs shall be protected from accidental or malicious deletion and modification.
- Paper copies of audit logs shall employed and distributed on a strictly need-to-know basis, shall be destroyed when no longer needed.

### **D. Audit Trail Reviews and Audit Storage**

Audit trails shall be reviewed as follows:

- For medium/highly critical servers on internal protected networks, on a weekly basis.
- For perimeter security intrusion detection systems on a daily basis, including firewall and IDS applications, daily.
- Following a known system or application software problem, a known violation of
- Existing policy by a user, or anomalous or suspicious system activity.

Audit trails shall be maintained on off-line archival media, at a minimum, for one year. Minimum online availability for auditable events will be 7 calendar days for those AIS that must, due to technical considerations, store those events locally. Minimum online availability for auditable events will be 90 days for those AIS and devices that log remotely to a centralized audit logging device. Reference the USPTO's Comprehensive Records Schedule for further instruction on audit log retention requirements.

### **E. Automated Tools**

To the maximum extent possible, audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, shall be used in real-time or near real-time. Audit analysis tools shall be used to help reduce the amount of information contained in audit trails, as well as to distill useful information from the raw data.

### **F. Monitoring of USPTO Network and AIS Activity**

USPTO networks and AIS shall be monitored for unauthorized or improper use.

Unauthorized or improper use of the systems shall be investigated and, when appropriate, official sanctions shall be imposed as a result of such use according the Office of Human Resource's Discipline and Penalties policy. If criminal activity is discovered, system logs shall be provided to the appropriate law enforcement officials.

The focus of network and AIS monitoring or auditing shall be predicated on identification and confirmation of behavior in violation of USPTO policy or federal law.

USPTO employees and contractor employees shall keep in mind that system may be accessible through legal discovery and the Freedom of Information Act (FOIA) and shall be maintained as records and protected as such.

## NETWORK AND AIS AUDIT, LOGGING, AND MONITORING POLICY

Only authorized local network and system administrators, auditors, and/or investigators for diagnostic and troubleshooting purposes and monitoring of misuse or malicious network activity will use network packet analyzers, or devices that operate in promiscuous mode.

### **G. Employee Investigations**

Requests for an employee investigation can be made by: 1) the supervisor, or a superior in the management chain of the employee to be audited with the approval of Executive Management, 2) the COTR of a contractor employee to be audited, 3) the Office of Human Resources or General Counsel, 4) higher authority Inspector General (IG), and 5) OCIO Operations management.

A record shall be maintained of user investigation requests and results.

Auditing can take place for any and all traffic on the network and AIS activity. All requests for log records related to employee misconduct (including Supervisors) shall be coordinated with Employee Relations and the Office of General Counsel or approved by the Director of the Network and Telecommunications Services Group.

### **H. Uniform Monitoring**

Network and AIS monitoring shall only be used to monitor activity on a system-wide level without the targeting of any specific person(s) until any suspected unauthorized activity has been identified. To ensure the integrity and objectivity of the network monitoring function, segregation of duties shall be maintained.

A user investigation report record shall be maintained for each individual investigation.

Precautions shall be taken to prevent, or decrease the risk of errors or irregularities with regard to data collection; identifying problems; and ensuring that the chain of evidence is preserved.

No single individual shall have control over all phases of network monitoring.

Approval for the collection, analysis, or use of the information gathered and the disclosure to law enforcement agencies, or other agencies outside the USPTO, shall be coordinated with Employee Relations or Office of the General Counsel, as appropriate, and approved by the Network and Telecommunications Services Group (NTSG).

### **I. Employee Notification and Privacy Expectations**

USPTO employees and contractor employees shall be notified on logical access to a USPTO IT system through a warning banner that must be agreed to or state that further use indicates consent to monitoring. This warning banner will state that all IT systems may be monitored and that unauthorized use will be grounds for disciplinary, civil or criminal proceedings.

USPTO employees and contractor employees do not have a right, nor should they have an expectation, of privacy while using any USPTO IT system at any time, including accessing the Internet or using e-mail. To the extent that USPTO employees and contractor employees wish that their private activities remain private, they should avoid using USPTO IT systems, the Internet or e-mail. By using USPTO IT systems, USPTO employees and contractor employees give their consent to disclosing the contents of any files or

## NETWORK AND AIS AUDIT, LOGGING, AND MONITORING POLICY

information maintained using USPTO IT systems to authorized USPTO staff. In addition to access by authorized USPTO staff, data maintained on USPTO IT systems may be subject to the legal process of discovery and Freedom of Information Act (FOIA) requests.

USPTO employees and contractor employees, by using USPTO IT systems, give implied consent to monitoring and recording with or without cause, including (but not limited to) their accessing the Internet or using e-mail. Any use of USPTO IT systems is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

USPTO employees and contractor employees shall not receive additional notification of specific monitoring actions of their usage unless the appropriate authority determines disciplinary action or criminal investigation is appropriate.

### **J. Implementation**

Specific implementation details for this policy may be located in the appropriate system security plan of a given AIS or documented in the operating system baseline configuration document.

### **K. Compliance**

Prohibited uses of USPTO AIS resources can result in administrative, judicial or non-judicial punishment in accordance with federal law and civilian employee regulations.

User Accounts shall be randomly audited to ensure compliance with established USPTO IT security standards. USPTO employee and contractor employee accounts shall be audited upon termination of employment and/or completion/termination of a contract.

Audit trail information is subject to the Freedom of Information Act (FOIA).

USPTO AIS, systems or applications that cannot meet established IT security standards shall be modified to remedy any deficiencies, where feasible. If compliance is not technically feasible then the System Owner of the AIS may defer compliance via a Plan of Action and Milestone entry with an expected date of compliance or a waiver of this policy may be requested. For waiver details please refer to the USPTO IT Security Handbook or similar policy instruction.

## **V. RESPONSIBILITIES**

All USPTO employees and contractor employees shall be aware of and observe the USPTO policy regarding network and AIS audit, logging, measurement, monitoring. All USPTO employees and contractor employees shall adhere to this policy and refrain from any activity that might circumvent this policy.

System Owners, Information System Security Officers, and System Administrators shall implement the mandatory practices of this policy for all USPTO AIS, systems, or applications they are responsible for.

The USPTO Enterprise Operations Center (EOC), in conjunction as operationally necessary with Information System Security Officers and/or ESSG staff, shall:

## NETWORK AND AIS AUDIT, LOGGING, AND MONITORING POLICY

- Log, monitor, and investigate possible security violations from activity involving access to and modification of sensitive or critical files.
- Review audit logs weekly for e-mail servers, medium and high criticality servers and hosts on the internal, protected network.
- Review audit logs from the perimeter security systems on a daily basis.
- Ensure the protection of system event logs with file-level permissions, segregation of duties, and all other safeguards commensurate with the highest level of sensitivity of the information resident on the system that the logs record data.
- When required, implement additional monitoring tools on critical servers as a supplement to the activity logging process provided by the operating system.

The USPTO IT Security Officer shall ensure that all systems have current and effective IT security plans that accurately reflect system status.

The USPTO Information Technology Security Management Group (ITSMG) shall:

- Maintain and update this policy, and monitor compliance through the conduct of annual compliance reviews.
- Ensure communication of the policy to all USPTO employees and contractor employees and will ensure that IT security awareness and training programs address network and AIS audit, logging, measurement, and monitoring.
- Be responsible for monitoring of system user compliance with this policy as part of the periodic IT security self-assessment program or automated system audits.

## **VI. EXCEPTIONS**

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

## **VII. 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.
- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- Federal Information Processing Standard (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.

## NETWORK AND AIS AUDIT, LOGGING, AND MONITORING POLICY

- OMB M-03-22 *Guidance for implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 2006.
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 2006.
- OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.
- OMB Memorandum 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*.

### **VIII. 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