



## UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

### REMOTE ACCESS POLICY OCIO-6005-09

**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. REFERENCES
- IX. EFFECT ON OTHER POLICIES

#### **I. PURPOSE**

This policy establishes the uniform policy within the United States Patent and Trademark Office (USPTO) to ensure that access to USPTO data from remote locations is provided to users in a secure and effective manner. This set of requirements defines a framework of implementation standards intended to protect USPTO IT networks, servers, and the data contained therein from the risks inherent in remote access without significantly impairing the USPTO mission or the quality of service to the remote user.

#### **II. AUTHORITY**

This policy is issued pursuant to:

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

#### **III. SCOPE**

The provisions of this policy apply to all USPTO employees and contractor employees accessing USPTO Automated Information Systems (AIS) and to contractor employees providing telecommunications and AIS services to the USPTO. This policy applies to all USPTO personnel (Federal and contractor employees) and all USPTO AIS or resources, independent of the size of the computer, network, device, or information. For example, it applies to desktops, laptops, servers, or other media that provides file or data storage. This policy also applies to those AIS operated and used by contractor employees, guest

## REMOTE ACCESS POLICY

researchers, collaborators, and other Federal agencies to carry out the USPTO mission, whether or not they are owned, leased, or on Government property. This policy is applicable to all equipment and systems used for remote access (e.g., laptops and workstations used to remotely access USPTO AIS from home, while on travel, or from other remote locations).

### **IV. DEFINITIONS**

**Authentication:** Authentication mechanisms provide an added level of assurance that users really are who they state they are. Authentication consists of something a user knows (such as, a password), something the user has (such as, a token or smart card), or something that is a part of the user (such as a fingerprint). It is the process by which the remote user is identified by entering a valid user name and password.

**Broadband:** Broadband is a type of data transmission in which a single medium (wire) can carry several channels at once [such as Digital Subscriber Lines (DSL) and cable TV/modem, two-way satellite, and other emerging technologies].

**Computer Security Incident:** A reportable incident consists of any act that violates an explicit or implied security policy within USPTO. More specifically, an incident is any adverse event that threatens the security of information resources. Incidents may include, but are not limited to:

- Compromise of integrity - when a virus, Trojan, or worm infects an AIS or network;
- Denial of service attack - when an attacker has disabled a network resource or a virus, worm, or Trojan has used all available network bandwidth;
- Loss of accountability/misuse - when an intruder or insider uses an account or an AIS for unauthorized or illegal purposes;
- Damage to any part of the AIS - when a virus, trojan, worm, or Federal employee or contractor employee destroys data; and
- Compromise of confidentiality/intrusion - when an unauthorized outsider gains access to our IT resources.

**Dial-up Access:** Dial-up Access is remote connectivity using a modem device to “call” other AIS over a public telephone line. Such access may utilize analog services, Integrated Services Digital Network (ISDN) service, or DSL telephone service.

**Firewall:** A firewall is a general term for a network perimeter or border router device (could be hardware, software, or both) designed to prevent unauthorized access to or from one networked environment to another networked environment. A computing environment may consist of one or more firewall devices that protect specific sensitive areas of the internal USPTO network. The outermost of these devices would face the public Internet. Firewalls can be configured to examine all messages entering or leaving a USPTO network and block those messages that are not explicitly allowed by the firewall configuration rules.

## REMOTE ACCESS POLICY

**Forensic Examination:** Forensic examination is the detailed inspection of computer memory and storage media to confirm or deny the occurrence of compromised information and applications, and if compromised, the extent to which information was compromised.

**Information Sensitivity:** Information sensitivity reflects the relationship between the characteristics of the information processed (e.g., personnel data subject to protection under the Privacy Act) and the mission need to ensure the confidentiality, integrity, and availability of the information (e.g., legal requirements to protect confidentiality of personal data). Sensitivity may vary from low to medium to high. During the AIS risk assessment, the System Owner must determine the sensitivity, or reaction, of the agency's mission to compromises of confidentiality, integrity, and availability of the information stored and processed by the AIS. This determination, along with the likelihood of compromise occurring, establishes the level of security adequate to protect the data as required by OMB Circular A-130, Appendix III. The System Owner must identify the management, technical, and operational controls necessary to provide the required protection.

**Local Area Network (LAN):** A computer network that spans a relatively small area, such as a single building or group of buildings.

**Personally Owned Resources:** Remote-access user owned computers, other hardware devices, and software.

**Public-Access Equipment:** Computers and other hardware devices that are owned by an entity or enterprise other than the USPTO or the remote user and allow unrestricted access by the general public.

**Remote Access:** Remote access uses telecommunications to enable authorized access to non-public USPTO computing services that would otherwise be inaccessible from work locations outside the established USPTO local area network or USPTO-controlled wide area network computing environment. This includes access to non-public USPTO AIS and data that are exposed to the public Internet (e.g., web access to electronic mail by the home user or business traveler), as well as modem dial-up and/or Virtual Private Network (VPN) access to internal USPTO IT servers and desktop workstations.

**Remote Location:** A work location where a worker is not able to connect a computer directly to the USPTO local area network or a USPTO-controlled wide area network that contains AIS needed for official duties. This includes a worker's home, a traveler's hotel room, or an emergency worker's field location. Work from remote locations requires the use of telecommunications capabilities, such as dial-up modems, Internet connectivity, or wireless networks to access USPTO AIS and data for official duty purposes.

**Remote user:** Any user who requires access to USPTO AIS from a remote location. Users may include USPTO Federal employees and contractor employees, employees of other Federal agencies who require remote access to USPTO AIS, and remote researchers processing USPTO information.

**Sanitization:** System sanitization is a process whereby the storage media (i.e. hard drive or USB drive) of a compromised system is "erased" in order to remove all traces of compromise or sensitive Government information.

## REMOTE ACCESS POLICY

**System Owners:** A project manager with day-to-day management and operational control over the AIS and direct oversight of the system/network administrators and operations staff. Although the Federal Government has ultimate ownership of all USPTO data, AIS and equipment, “owner” is the term commonly used by the National Institute of Standards and Technology (NIST) to refer to individuals with specific AIS oversight responsibilities. The “System Owner” role is discussed at length in the C&A section of the IT Security Handbook.

**Telework/telecommuting:** Telework or telecommuting occur when authorized USPTO employees perform all, or a part of, their work away from their normal places of business, usually at home or from an established Government telework center.

**USPTO-owned/furnished resources:** USPTO-owned/furnished resources including computers, other hardware devices, software, and data provided to remote users for use in their official duties.

**Virtual Private Network (VPN):** A virtual private network is a private “tunnel” through a public network (i.e., the Internet). For example, there are a number of systems that can establish private networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

**Wide Area Network:** A wide area network consists of the connection of many LANs over any distance via telephone lines and radio waves.

**Wireless LAN (WLAN):** A wireless LAN consists of a network that uses radio waves rather than wires to communicate between nodes.

## V. POLICY

The following minimum standards apply to all USPTO federal employees and contractor employees who remotely access unclassified USPTO AIS, as well as other authorized Government officials, business partners, third party collaborators, and researchers who require remote access to USPTO AIS. This policy applies to all USPTO AIS, regardless of platform, that allow such access, and it explains the proper configuration and maintenance of the devices used to conduct remote access, including USPTO-owned/furnished, personally owned, and publicly accessed equipment, as well as equipment at alternate operation sites used for continuity of operations activities. This policy applies to contractor employees as provided for in USPTO contracts.

This policy applies to all AIS and its authority is independent of the type of remote access technology. This policy includes the following modes of remote access: modems, broadband and wireless connections; third party Internet service providers (ISP); public access sites such as kiosks and Internet cafés; and alternate platforms such as personal electronic devices (PED)/personal digital assistants (PDA); and cell phones. It applies to all AIS used to carry out the USPTO’s mission, located both on and off Government property, whether operated by Federal employees or contractor employees.

All USPTO Remote Access Users, including USPTO Federal employees and contractor employees, must follow the mandatory minimum standards of this policy. Failure to comply with this policy may result in disciplinary action and/or revocation of remote access privileges.

## REMOTE ACCESS POLICY

Remote users shall:

- Complete initial and annual refresher IT security awareness training as required by USPTO IT security policy.
- Certify that the user has read and understand their responsibilities under this policy prior to receiving remote access authorization and authentication credentials. Adhere to the terms of signed “remote access user security agreement” or similar agreement (See Appendix A).
- Ensure the computer used for remote access is configured and maintained according to this policy and according to the method of remote access being used. (See Appendix B -- Minimum Standards for Protective Remote Access Countermeasures).
- Periodically check to determine that all applicable configuration guidance and security patches available for the software used to process USPTO information on personally owned computers have been installed.
- Return USPTO-owned computers used for remote access, as required and as directed by the responsible manager, supervisor, COTR, or ISSO, so that the security configuration (e.g. patches) of the computer can be checked and updated.
- Exercise caution when accessing Government information from a public area to prevent compromise of sensitive information by inadvertent “over the shoulder” reading of material.
- Report within 24 hours of identification all IT security incidents to their supervisor, to their COTR, to their ITSO, or to the USPTO CIRT following USPTO incident reporting procedures.

All USPTO System Owners must determine the sensitivity of information contained in their AIS as part of the decision-making process to allow or deny remote access to data on their AIS. System Owners must also ensure that: remote access controls are implemented consistently with the risk and magnitude of harm to the information and the mandatory minimum standards of this policy; the relevant AIS security plans document the types of remote access that are acceptable and document the security controls required for that access; and ensure the relevant system security plan includes approved waivers of the requirements of this policy. The waiver process is detailed in the IT Security Handbook.

USPTO categorizes remote access into three tiers, according to the risk of harm inherent in the nature of the access and the sensitivity of the information accessed.

Tier 1 represents low risk because the AIS accessed are between the outermost USPTO network perimeter or border device, such as the USPTO firewall, and outside inner USPTO firewalls that protect local area networks. In addition, Tier 1 information is of low sensitivity.

Tier 2 represents medium risk because basic user privileges are allowed to access AIS processing or storing sensitive-but-unclassified information inside the inner USPTO firewalls and internal to the USPTO computing environment.

## REMOTE ACCESS POLICY

Tier 3 represents high risk because administrative (or “super-user”) privileges are allowed to access AIS processing or storing sensitive-but-unclassified information that are internal to the USPTO computing environment.

### **VI. RESPONSIBILITIES**

All USPTO employees and contractor employees shall adhere to this policy and to refrain from any activity that might circumvent this policy.

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, if necessary, must identify any proposed deviations from the mandatory practices of this policy and request a waiver in writing from the USPTO IT Security Officer in accordance with the waiver process as defined in the USPTO IT Security Handbook.

System administrators shall ensure technical controls and/or operational procedures are in place to identify, prevent, correct, and report violations of this policy. Violations of this policy shall be reported via e-mail to the HELPDESK 9000 e-mail address.

The IT Security Management Group (ITSMG) shall maintain and update the policy annually, review and approve or deny waivers, and monitor compliance through the conduct of annual compliance reviews.

ITSMG shall be responsible for the monitoring of AIS user compliance with this policy as part of the periodic IT security self-assessment program or AIS evaluations, and maintaining approved waivers as part of the documentation for appropriate system security plan(s).

ITSMG shall ensure communication of the policy to all USPTO employee and contractor employee AIS users and shall ensure that IT security awareness and training programs address the proper use of remote access privileges.

### **VII. EXCEPTIONS**

1. This policy does not apply to remote access of publicly accessible USPTO Web sites, such as [www.uspto.gov](http://www.uspto.gov), including those USPTO sites intended to provide services to the public that support transactions and access to databases although the access supports official Government business.
2. The term "remote access" as used in this policy does not include such public Web site access, except when the public access site supports access to AIS and data not publicly available through such Web. This would be the case if a USPTO public Web site provided initial access for a secure portal that required further authentication for access to internal resources.
3. This policy does not cover requirements for securing the servers and applications that are remotely accessed.

Additional exceptions to this policy shall be determined on a case-by-case basis using the waiver process as defined in the USPTO IT Security Handbook.

## REMOTE ACCESS POLICY

### **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.
- 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.
- 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*.

### **IX. EFFECT ON OTHER POLICIES**

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

REMOTE ACCESS POLICY

ISSUED BY:



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

OFFICE OF PRIMARY INTEREST: IT Security Management Group