



governmentattic.org

"Rummaging in the government's attic"

Description of document: The United States Patent and Trademark Office (USPTO)
Rules of the Road, 2012

Requested date: 08-August-2012

Released date: 23-August-2012

Posted date: 10-September-2012

Title of document USPTO Rules of The Road, OCIO-POL-36

Source of document: **USPTO FOIA Officer**
United States Patent and Trademark Office
PO Box 1450
Alexandria, VA 22313-1450
Email: efoia@uspto.gov

Note: This is generally guidelines for USPTO employees on appropriate use of the Internet.

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE GENERAL COUNSEL

August 23, 2012

Re: Freedom of Information Act (FOIA) Request No. F-12-00199

The United States Patent and Trademark Office (USPTO) FOIA Office received your e-mail dated Wednesday, August 08, 2012, in which you requested, under the provisions of the Freedom of Information Act, 5 U.S.C. § 552:

A copy of the USPTO's Rules of the Road.

The United States Patent and Trademark Office identified one document that is responsive to your request. A copy of this material is enclosed.

Your request is considered completed with full disclosure. However, you have the right to appeal this initial determination to the General Counsel, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. An appeal must be received within 30 calendar days from the date of this letter. See 37 C.F.R. § 102.10(a). The appeal must be in writing. You must include a copy of your original request, this letter, and a statement of the reasons why the information should be made available and why this initial determination was in error. Both the letter and the envelope must be clearly marked "Freedom of Information Appeal."

The processing fee was less than \$20.00, and is hereby waived.

Sincerely,

Kathryn Siehndel

Kathryn Siehndel
USPTO FOIA Officer

Enclosure



UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

USPTO RULES OF THE ROAD OCIO-POL-36

Effective Date: May 21, 2012

Purpose of Revision: Revised rule for saving Federal records; clarification of employee use of the Internet

Review Date: May 17, 2012

Version: 3.0

TABLE OF CONTENTS

Section

- I. Purpose
- II. Authority
- III. Scope
- IV. Policy
- V. Responsibilities
- VI. Effect on Other Policies
- VII. References

I. PURPOSE

The PTONet, USPTO Wireless Network, USPTO Automated Information Systems (AISs), and other computing resources are shared among USPTO employees. PTONet provides access to USPTO business systems that operate on the USPTO information technology infrastructure and provides access to remote information systems through secure gateways.

This *Rules of the Road* policy document is intended to help you use the USPTO's computing and network facilities responsibly, securely, and efficiently, thereby maximizing the availability of these facilities to all employees.

Complying with these rules will help maximize access to these facilities and help ensure that your use of them is responsible, legal, and respectful of privacy. You must follow the Rules of the Road when using USPTO automation resources.

The Rules of the Road are grouped into three categories to ensure users comply with:

1. The intended use of USPTO resources.
2. The ethical use of USPTO resources.
3. The proper use of USPTO resources.

USPTO RULES OF THE ROAD

The following is a more detailed discussion of the individual rules associated with each category. The Rules of the Road are also discussed in appropriate sections of various User Guides offered by the OCIO Service Desk, including the USPTO Internet and Intranet Services Guide and the USPTO E-Mail User's Guide. Each USPTO Business Unit may supplement the Rules of the Road for better administration of information within its own organization. The Office of Human Resources Policies and Procedures include employee guidelines for the USPTO workplace. Other USPTO directives can be found at <http://ptoweb/ptointranet/directives/index.html>.

II. AUTHORITY

This policy is issued pursuant to:

- *The Federal Information Management Security Act of 2002 (FISMA)*
- *OCIO-1001-09 Policy Management*

III. SCOPE

The provisions of this policy are written towards and apply to **all USPTO employees and contractor employees** using or operating USPTO computer systems, and to **employees of contractor systems** owned and operated on behalf of the USPTO.

IV. POLICY

Complying with the Intended Use of USPTO Resources

It is important that you understand the purpose of PTONet, USPTO Wireless Network, and any USPTO Automated Information System (AIS) that you use so that **your use of these systems conforms to their intended purpose** and is in compliance with applicable policies.

Rule #1: Do not conduct unauthorized business on USPTO resources

The purpose of the USPTO is to administer the laws relating to patents and trademarks in order to promote industrial and technological progress in the United States and strengthen the national economy. As a USPTO employee, you have an obligation to conduct your activities in keeping with the USPTO mission, goals, and objectives. All use of PTONet, USPTO Wireless Network, and USPTO AISs, including accessing the Internet, must be consistent with this purpose. The following are appropriate uses of USPTO resources:

- Exchange of information that supports the USPTO mission, goals, and objectives.

USPTO RULES OF THE ROAD

- Job-related professional development for USPTO management and staff.
- Communications and exchange of information intended to **maintain job currency** or **gain additional knowledge that is directly or indirectly related to job functions.**
- Communications and exchange of information generally supportive of otherwise acceptable uses.

Internet services and e-mail provided by the USPTO are intended for authorized purposes during business hours. However, limited personal use of the Internet, including **sending infrequent personal e-mail messages, is permissible** provided such use is consistent with the Rules of the Road and does not interfere with conducting USPTO business. Use of certain tools, such as WebEx, should be restricted to Official Business only, given their unique nature and potential for negative impact on PTONet. The privilege to use government equipment for limited personal purposes may be revoked or restricted at any time by the USPTO. USPTO employees should consult with their supervisors in case of any doubt about the appropriate use of any government equipment. Please refer to the USPTO policy *AAO 202-735 Limited Personal Use of Government Equipment* and *USPTO Terms of Wireless Service Use* for further details.

The USPTO flexible work schedules, including the Increased Flextime Policy (IFP) and mid-day flex (see *Office of Human Resources Administrative Policies*) should minimize the necessity for personal use of any and all government equipment during official working hours. However, employees are reminded of their obligation to truthfully certify their time and attendance records and to report as duty-time only that time spent performing official duties.

All unauthorized use of USPTO resources is prohibited. The following activities, while not an exhaustive list, are specific examples of **unacceptable uses** of the PTONet, USPTO Wireless Network, and USPTO AISs:

- Using resources for **commercial purposes**, for **financial gain**, or in support of **private business** activities.
- Initiating actions that interfere with the supervisory or accounting functions of the AIS, including attempts to obtain elevated privileges without proper authorization.
- Creating, storing, or sending electronic chain letters.
- Using the Internet or intranet as a staging ground or platform to gain unauthorized access to other systems.
- Creating, storing, or sending electronic chain letters.
- Publishing personal opinions to external (non-USPTO) entities while using a USPTO Internet user-ID without express authorization based on individual job description or through other USPTO clearance process. (Inclusion of a disclaimer that such statements are not those of the USPTO is not sufficient to obviate or negate this restriction.)

USPTO RULES OF THE ROAD

- Any communications with the media without prior approval of the Office of the Chief Communications Officer. For guidelines, refer to the USPTO Media, Press, and Social Media Policy.
- Engaging in any activity that would discredit the USPTO, including the creation, downloading, viewing, storage, copying, or transmission of sexually explicit and/or sexually oriented materials or materials related to gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited.

In the normal course of operations and maintenance activities, usage may be monitored in order to ensure the continued operational effectiveness and integrity of the PTONet, USPTO Wireless Network, USPTO AISs, and other computing resources. You are reminded that such monitoring does occur. Unauthorized or improper use of the AIS will be investigated, and when appropriate, official sanctions will be imposed as a result of such use. If criminal activity is discovered, information will be provided to the appropriate law enforcement officials.

Rule #2: Save Federal Records

The Federal Records Act defines records as “all books, papers, maps, photographs, or other documentary materials, regardless of physical form or characteristics, received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included.” (44 U.S.C. 3301).

Any electronic message (e.g., information transmitted through electronic mail, the Internet, or wireless hand-held device) should be treated as if it were a paper document when it comes to determining whether it is a Federal record.

Federal records must be maintained according to an approved disposition schedule. Refer to the Comprehensive Records Schedule for the USPTO.

Use the following guidelines to determine if a document (electronic or hard copy) should be considered a Federal record:

- If you take official action related to a message, it is a federal record.
- If the message is needed for adequate and complete documentation of an action you have taken or has been taken in the course of your business, it is a federal record.

You must maintain the body, subject, date transmitted and names of the sender(s) and receiver(s). You also must maintain attachments to an electronic message if that message is a federal record. Federal records must be managed in a proper record keeping system.

USPTO RULES OF THE ROAD

Where an electronic record keeping system exists, the electronic message or electronic mail record should be retained in that system.

If you have any questions about the determination or disposition of an electronic message, or need assistance in managing electronic records, please contact your Business Area's records coordinator or the USPTO Records Officer.

Complying with the Ethical Use of USPTO Resources

The opportunities that PTONet, USPTO Wireless Network, and USPTO AISs provide for USPTO employees to share information, come with the responsibility to use the AISs in accordance with USPTO standards of conduct. These standards are described in the IT security awareness training that all employees are required to take annually in accordance with *OCIO-6009-09 IT Security Education Awareness Policy*. Appropriate use of PTONet, USPTO Wireless Network, and USPTO AISs includes maintaining the security of the AISs, protecting privacy, and conforming to applicable laws, particularly copyright and harassment prevention laws.

Rule #3: Do not let anyone know your password

While you should feel free to let others know your username (this is the name by which you are known to the whole PTONet, USPTO Wireless Network, USPTO AISs and Internet community), you should never let anyone know your account passwords. This includes trusted friends.

Giving someone else your password is like giving them a signed blank check, or your charge card. You should never do this, even to "lend" your account to them temporarily. Anyone who has your password can use your account, and whatever they do that affects the AIS will be traced back to your username — if your username or account is used in an abusive or otherwise inappropriate manner, the USPTO will hold you responsible.

When creating or changing your password, always use a password that you can easily remember but is unique enough that it cannot be easily guessed by your co-workers. Never use the names of spouses, children, pets or birthdates, as these can easily be compromised.

USPTO operates a few systems which require shared accounts/passwords, i.e., ENews, IdeaScale, to allow duties to be shared among system admins. These are exceptional cases, requiring supervisor permission.

Rule #4: Do not violate the privacy of other users

The *Electronic Communications Privacy Act* (18 USC 2510 et seq., as amended) and other Federal laws protect the privacy of users of wire and electronic communications. The facilities of the PTONet, USPTO Wireless Network, and USPTO AISs are in place to facilitate the sharing of information among USPTO employees, our international partners, and our customers. As a user of USPTO resources, make sure that your actions do not violate the privacy of other users, even if unintentionally.

Some specific areas to watch for include the following:

USPTO RULES OF THE ROAD

- Do not try to access the files or directories of another user without clear authorization from that user.
- Do not try to intercept or otherwise monitor any network communications not explicitly intended for you.
- Do not use names or other personal identifiers in communications that might be of a sensitive or confidential nature.
- Do not intentionally seek information about, browse, obtain copies of, or modify files, mail, or passwords belonging to others, whether they are at the USPTO or elsewhere, unless specifically authorized to do so by those individuals.
- Do not attempt to decrypt or translate encrypted material belonging to another person or organization.
- Do not attempt to alter the “From” line of your PTOnet user-ID or other attributes of origin in electronic mail, messages, or news group postings.
- Do not create any shared programs that secretly collect information about USPTO users.

Rule #5: Do not transmit classified or sensitive data

Every attempt has been made to ensure that appropriate security mechanisms are in place for protecting information from unintended access, from within the AIS or from the outside. However, these mechanisms, by themselves, are not sufficient. PTOnet, USPTO Wireless Network, and USPTO AIS users should ensure that they take appropriate action to safeguard classified or sensitive data. All USPTO users are instructed to implement the following requirements:

- Do not transmit classified data, data subject to a secrecy order, or data under seal through the Internet or e-mail, unless it has been properly protected through encryption software.
- Do not store or transmit sensitive data without proper protection as defined in applicable Federal laws and regulations. Sensitive data should be safeguarded during collaboration sessions and should not be posted in open discussion groups or other social media sites. Data should be considered sensitive if it might be exempt from *Freedom of Information Act (FOIA)* disclosure or protected under *The Privacy Act*. Sensitive data includes records about individuals in which there is a reasonable expectation of privacy, trade secrets or confidential business information, and confidential information related to Patent and Trademark applications.
- Do not transmit data that is part of the USPTO internal decision-making process over the Internet or in public news groups.
- Do not automatically forward electronic mail, via rule, macro, or script to an address outside the USPTO network. Automatic forwarding potentially creates a serious operational threat and

USPTO RULES OF THE ROAD

an unjustified risk to confidentiality obligations. Sensitive USPTO information may inadvertently be transmitted and stored in a public medium without protection. Senders using automatic forwarding have no knowledge or control of the content that is being forwarded and have no way to filter sensitive information from being forwarded. Therefore, auto forwarding of e-mail outside the USPTO network is prohibited. Auto-replies or out-of-office settings, which do not use auto-forwarding, are **not** prohibited. The following are examples of sensitive data that should not be discussed or transmitted on PTOnet or related computing services:

- Anything with sensitive personnel data such as names with Social Security numbers, leave balances, salaries, or benefits for which an employee is signed up.
- Anything dealing with the details surrounding an Employee Relations or Union issue.
- Sensitive procurement information (any procurement in the \$1 million or over category, not purchase orders).
- Anything dealing with the details surrounding contract award prior to an award.
- All information categorized as Source Selection Information by Section 27 of the *Office of Federal Procurement Policy Act* (41 U.S.C. 423) that concerns the number, identity, ranking, or evaluation of offerors in response to an ongoing procurement action.
- Information marked by an offeror as proprietary.
- Source selection information, including bid prices prior to bid opening, proposed costs/prices in response to a solicitation, source selection plans, technical evaluation of proposals, cost or price evaluations, competitive range determinations, ranking of offers, and reports or evaluations of source selection panels.
- Anything dealing with budget policy prior to the budget submission, particularly as it may deal with USPTO employees.
- Passwords or other computer security related items.

Rule #6: Do not copy or misuse copyrighted material, including software

The use of the PTOnet, USPTO Wireless Network, and USPTO AISs, including the ability to access external information through the Internet, offers you an opportunity to more effectively perform your job. This expanded capability emphasizes the need to be aware of copyright restrictions. Many computer programs and related materials, such as documentation, are owned by individual users or third parties, and are protected by copyright and other laws, together with licenses and other contractual agreements. Copyright considerations also apply to some of the non-computer related documents that are obtainable through the USPTO's access to the Internet. **Failure to abide by legal and contractual restrictions on the use of copyrighted products could make you subject to civil and criminal prosecution.** Therefore, you should observe the following restrictions:

USPTO RULES OF THE ROAD

- Copyrighted and licensed materials, including software, should not be used on USPTO AISs or collected or disseminated via PTONet, USPTO Wireless Network, or distributed through e-mail or other collaboration systems **without the copyright or license owner's approval.**

Rule #7: Do not use USPTO resources to store or transmit offensive material or harass anyone in any way

The USPTO is proud of its efforts to create a work environment free from all forms of harassment. As a PTONet, USPTO Wireless Network, and USPTO AIS user, you should not use these resources in any way that unreasonably interferes with anyone's work or creates an atmosphere where others feel harassed. You should not use any USPTO resources to convey obscene, profane, discriminatory, abusive, or otherwise offensive material. Any USPTO employee who feels harassed should seek assistance and resolution of the complaint. To report any such abuse, contact the Service Desk at (571) 272-9000.

Complying with the Proper Use of USPTO Resources

PTONet, USPTO Wireless Network, and USPTO AIS resources, as well as news groups, mail servers, and Internet resources accessible through PTONet, are powerful tools that can easily be misused.

Rule #8: Do not overload USPTO resources or abuse the network

In order for the USPTO to obtain maximum use of its PTONet, USPTO Wireless Network, and USPTO AIS resources, you should carefully evaluate your use of these resources and not overly tax processing and storage capabilities in a manner that restricts access by other users. You are required to observe the following:

- Avoid sending e-mail attachments larger than 10 megabyte. This is a document of approximately 30 pages if it is straight text. If graphics or spreadsheets are included, you could reach 10 MB in as little as one page. See the *USPTO E-Mail User's Guide* for information on sending attachments.
- Limit streaming or download of audio and video files. Media-rich communications take up significant resources and can increase bandwidth consumption in a manner that negatively affects our ability to carry out mission-critical functions. While you may use media-rich videoconferencing systems and other collaborative tools for official business purposes, you should notify your supervisor in advance if you have a need to download or stream media files for other purposes. Usage will be monitored. Streaming or downloading games, movies, or videos for entertainment purposes is never permitted.
- **Archive e-mail messages you need to keep after you have read them.** Delete mail you have read but no longer need, and delete old messages and unneeded documents out of file folders.
- Do not send broadcast messages (i.e., messages addressed to a server and/or to all users). Instead, for messages that must be widely disseminated, use authorized collaboration sites,

USPTO RULES OF THE ROAD

shared folders, or an Intranet page. The Office of the Chief Communications Officer can assist in coordinating agency-wide messages when appropriate.

- Do not develop unauthorized Scripts, Macros, Web Crawlers, Utilities, Local Applications or other software or batch processes to automate tasks that are run on or are executed against workstations, servers or other network resources. Unauthorized automation of tasks has the potential of adversely impacting AIS availability by significantly impacting its performance and availability. Solutions to automated tasks need to be designed carefully by authorized persons in OCIO or business executive management in accordance with USPTO System Development Life Cycle (SDLC) processes to prevent these occurrences. Under certain circumstances, you may be authorized to perform limited automated processes on your local workstation or collaboration site, as afforded by your access rights. Refer to the policy on Application Development by End Users for additional information.

Rule #9: Use proper e-mail etiquette

You are authorized and encouraged to communicate with others using the USPTO's electronic mail (e-mail) service whenever appropriate. The use of e-mail enhances your ability to reach an intended message recipient; saves time; provides enhanced search, retrieval, and filing capabilities; and makes electronic records available to many users simultaneously. You are encouraged to observe the following practices:

- Keep your messages as brief and to the point as possible.
- Always fill out the subject line. Give a brief, clear description of the message.
- When sending messages to a group, ask yourself "Does everyone in this group need to see this message?"
- Be careful with humorous or witty messages. If sent to people who know you, most likely they will understand your meaning. To strangers, your message may be interpreted as offensive. Assume your message might someday be requested under FOIA or the Privacy Act.
- Your messages should not contain any obscene, profane, discriminatory or otherwise offensive material.
- Some people view upper case or very large or red fonts as the equivalent of shouting. Be aware of the potential to unintentionally cause offense.

Remember that once your message is sent, you cannot take it back and it is out of your control. It can be printed or forwarded to others.

Rule #10 Conduct virtual meetings responsibly

New types of collaboration tools are designed to promote meeting efficiency through information sharing and voice and video communications among campus-wide users, telecommuters working at remote

USPTO RULES OF THE ROAD

locations, and external contacts around the globe. Awareness of key aspects of virtual meetings will help foster a positive experience and protect information from unintended disclosure.

- Use care to protect systems and sensitive information during videoconferences and other collaboration sessions. Desktop sharing and peer-to-peer file transfers are both prohibited across the Internet.
- If you are hosting a virtual meeting that is being monitored or recorded, you must provide notification to all participants. Similarly, you should be alert to ensuring that proper notification is provided when attending a meeting that is being hosted and recorded by other entities.
- If you are hosting a virtual meeting with speaker-phones or other audio capabilities, you should take care to identify the names of participants and/or number of people listening in.
- As with in-person meetings, be vigilant against inappropriate comments and offensive materials.
- Whether you are hosting or attending a meeting, take precautions to ensure that unauthorized participants do not gain access to the collaborative session audio, video, or data (e.g. attending a WebEx meeting while in a public space, using a mobile device that may provide unauthorized access).
- Do not forward collaborative meeting invitations to unauthorized parties.
- Do not connect to a collaborative conversation that you were not invited to.
- Be prepared. Know how to operate the tools to conduct a virtual meeting and practice ahead of time. For large meetings, prepare materials in advance and have a contingency plan for any disruptions. For further details, see the [Virtual Collaborative Tools](#) site on the USPTO Intranet.

Rule #11: Do not compromise the integrity of USPTO resources

Computer viruses represent a significant threat to the operational readiness of PTOnet, USPTO Wireless Network, and USPTO AISs. Given the USPTO's increasing dependence on the information processed and stored on AISs, it is important that you understand and recognize the basic threat that a computer virus represents. You must learn how to protect against virus infections, detect their presence, and obtain assistance to repair the damage they cause. While there are no easy answers to these problems, you can create a preventive and protective atmosphere by implementing the following safeguards:

- Use only U. S. Government acquired software obtained through proper USPTO distribution or requisitioning channels.
- You are prohibited from unauthorized acquisitions, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes

USPTO RULES OF THE ROAD

privacy information, copyrighted, trademarked or material with other intellectual property rights (beyond fair use), proprietary data, or export-controlled software or data.

- You are prohibited from transferring and installing any software product, including public domain freeware or shareware, across the PTOnet, USPTO Wireless Network, via the USPTO's e-mail AIS or downloading software products from external sources, including the Internet, unless the software has been tested and approved by the Office of the Chief Information Officer.

Rule #12: Protect PTOnet and USPTO AIS assets

The USPTO has invested considerable time and money to establish an automation environment that provides you timely access to the computing resources and information you need. In order to ensure that you continue to receive the services you require, certain actions must be taken to protect USPTO automation assets:

- Do not reconfigure USPTO computer hardware and software assets without prior approval. This includes adding privately owned hardware items or software packages to the standard USPTO baseline configurations.
- Do not modify system files without permission of the Office of the Chief Information Officer. Modification includes deliberate editing, changing, adding, or deleting of program codes within a system file. This modification restriction does not prohibit you from changing system files as a result of changing desktop parameters, network printer selections, etc., through the desktop operating system environment.
- Use care when eating or drinking near USPTO computers. Food crumbs and spilled drinks can cause damage to computer components.
- Safeguard your data by limiting unauthorized access to PTOnet resources and files.
- Never attempt to cut, break or remove any lock or physical security device attached to any Government-owned microcomputer, printer, or other information technology equipment.
- Do not try to perform your own repairs or move your computer or other information technology equipment for any reason. Call the Service Desk at (571) 272-9000 if your computer is malfunctioning or needs to be moved. Hardware upgrades must be approved in advance. See the *USPTO Guide to Acquiring IT Desktop Hardware* for the approval process.
- Check the placement of your computer, monitor and other electronic computer equipment to make sure that air vents are not blocked or covered. An obstructed flow of air can cause the equipment to overheat and malfunction.
- It is every USPTO employee's and contractor employee's responsibility to report actual or suspected computer incidents and possible virus infections as soon as they occur. You can report all incidents and virus infections to the CIO Command Center (C3) by calling

USPTO RULES OF THE ROAD

(571) 272-6700 or by e-mail to CIOcommandcenter@USPTO.GOV or ABUSE@USPTO.GOV e-mail addresses from within USPTO or from remote locations. Do not send an e-mail to C3 or anyone else from the infected workstation. C3 is staffed 24 hours a day. Please leave a voice message with sufficient detail to identify the nature of the incident and a means to contact you if C3 is unable to answer the phone. Computers that are suspected of being infected by a computer virus should be disconnected from the network immediately, remain powered on and attended by someone to prevent others from using the AIS until a member of C3 arrives. AISs should be disconnected from the network by removing the network cable from either the end that is connected to the network interface card (NIC) in the computer or from the end that is plugged into your network wall jack.

Rule #13: Be mindful of your mobile environment

- Keep in mind that in a mobile environment people could be watching as you enter your password, and/or perform work. Be mindful of your surroundings while working on a mobile device in a public area. Individuals can attempt to obtain sensitive information by shoulder surfing.
- If you're working in an environment where someone could be standing behind you watching your activities, move to a location where your work cannot be seen by prying eyes.
- Access from public wireless access points and networks increases risk to individual users and should be avoided.

Rule#14: Do not attempt to circumvent security controls.

- The USPTO has implemented security controls to prevent inappropriate access and monitor traffic. All users should be aware of the restrictions in place and never attempt to circumvent these controls. Any attempt to circumvent the implemented security controls will be viewed as malicious activity on the network.
- Do not attempt to connect unauthorized devices to the Enterprise Wireless (PTOPRIVATE) network. Only a PTO-provided Universal Laptop is authorized to connect to the Enterprise Wireless network, which requires using Login ID, password, and USPTO provided smartcard. The UL device is not authorized to access both wireless connection and direct connection to USPTO's internal network at the same time. The wireless service is not to be connected to the USPTO wired internal network. The USPTO may terminate, modify, limit use of, make changes to, or modify the Terms of Service of this capability at any time without notice.
- You can connect to PTOPUBLIC via a personally owned portable device such as a laptop computer, IPAD, or PDA.

Rule#15: Be mindful of special requirements when traveling abroad on USPTO business

USPTO has a responsibility to be extraordinarily vigilant in safeguarding intellectual property along with the processes and information related to granting IP rights, especially when traveling in foreign countries. In light of this responsibility the CIO staff has taken steps to be extra diligent in securing the IT technology that accompanies our employees who engage in foreign travel. Please be mindful of these policies and procedures:

- All USPTO travelers must certify they have read the “Defense Travel Briefing” at least annually. The briefing is available via the USPTO Intranet, on the Security/Safety Web page, under the “What’s New” section of the page.
- Travelers must adhere to all guidelines in USPTO’s *OCIO-6001-09 Information Security Foreign Travel Policy*.
- Access to PTO network resources and systems from foreign countries is generally prohibited unless approved in advance. To obtain permission for unclassified, remote access from a foreign location, all travelers must fill out the “User Agreement for Remote Access from Foreign Locations” form found in Appendix A of USPTO’s *OCIO-6001-09 Information Security Foreign Travel Policy*. **The form must be filled out by the traveler, and signed by the supervisor.** Refer to USPTO’s *OCIO-6001-09 Information Security Foreign Travel Policy* for further details when there is a requirement for access while on official travel.
- Only USPTO equipment issued for foreign travel, Overseas Travel Equipment (OTE), may be used for conducting USPTO business overseas; no personal devices may be used for this purpose. Any laptops that are designated for overseas use include full disk, sophisticated encryption and automatic virus scanning for any removable devices mounted on it, such as memory cards, flash drives and similar equipment. In special circumstances, when there is an over-riding need for an employee to use their normal, everyday USPTO equipment overseas, the CIO staff can specially configure such equipment for business use outside of the United States. This is a significant effort, and we prefer you use pre-configured OTE. The CIO asks that you request OTE 72 hours (three business days) prior to your departure date.
- USPTO equipment both leaving and returning from foreign travel will be security-scanned at check-out and turn-in, including an employee’s USPTO-owned Blackberry that has been issued for daily use.
- Staff must ensure that no intellectual property or personally identifiable information is stored on overseas travel equipment.
- **Employees should use only the USPTO-established ‘alias’ e-mail account**, through VPN, while overseas. The use of regular USPTO Outlook Web Access is explicitly prohibited.

USPTO RULES OF THE ROAD

- Personnel should secure equipment in locked storage when it is not directly under the person's control, for instance when attending a social activity with foreign colleagues. Equipment should be in carry-on luggage when in transit.
- Travelers shall not allow unauthorized access to USPTO equipment by foreign representatives.
- It is also recommended that no removable media obtained from foreign sources be mounted on USPTO equipment (e.g. flash drives, memory cards, etc.). Occasionally, there might be a compelling business need to do this in the spirit of collaborating with foreign colleagues; but, in general, it is discouraged. When in doubt, consult with your supervisor.
- USPTO-issued OTE is not authorized for employees' use during personal foreign travel. For instance, if a staff member takes annual leave at the conclusion of a foreign USPTO business trip to do pleasure traveling, the use of OTE is prohibited
- Upon return from travel, travelers must turn removable media into the USPTO Computer Incident Response Team (CIRT) for forensic analysis and sanitization or destruction, as required.

For full details on the requirements for foreign travel, refer to the USPTO's *Information Security Foreign Travel Policy*.

V. **RESPONSIBILITIES**

The provisions of this policy apply to all USPTO employees and contractor employees using or operating USPTO computer systems, and to employees of contractor systems owned and operated on behalf of the USPTO.

VI. **EFFECT ON OTHER POLICIES**

This policy affects all new, revised, or retired policies issued in Fiscal Year 2012.

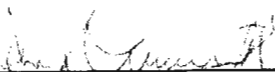
VII. **REFERENCES**

- 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.

USPTO RULES OF THE ROAD

- 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. September 30, 2003
- 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, Information Security Security Program Policy, January 2009
- U.S. Patent and Trademark Office IT Security Handbook.
- U.S. Patent and Trademark Office IT Privacy Policy.
- U.S. Patent and Trademark Office Comprehensive Records Schedule.

ISSUED BY:



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

OFFICE OF PRIMARY INTEREST: Office of Organizational Policy and Governance