USPTO RULES OF THE ROAD
OCIO-POL-36

Effective Date: May 21, 2012
Last Revision Date: October 29, 2019
Purpose of Revision: Annual review and updates of outdated information including references and links.
Version: 6.0

TABLE OF CONTENTS

Section

I. PURPOSE

The PTOnet, United States Patent and Trademark Office (USPTO) Wireless Network, USPTO information systems, 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.

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

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.

The following is a more detailed discussion of the individual rules in each category. 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 on the list of agency directives.

II. AUTHORITY

This policy is issued pursuant to:

- The Federal Information Management Security Act of 2002 (FISMA)
- Federal Information Security Modernization Act of 2014 (FISMA)
- Federal Information Technology Acquisition Reform Act (FITARA)
- OMB Memorandum M-15-14, Management and Oversight of Federal Information Technology
- OCIO-1001-09, Policy Management

III. SCOPE

The provisions of this policy are written for 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 to understand the purpose of PTOnet, USPTO Wireless Network, and any USPTO information systems that you use so that your use of these systems conforms to their intended purpose and complies 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 alignment with the USPTO mission, goals and objectives. All use of PTOnet, USPTO Wireless Network, and USPTO information systems, 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.
- 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 email provided by the USPTO are intended for authorized purposes during business hours. However, limited personal use of the internet, including sending infrequent personal email 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, Employee WiFi quick Reference Guide, and Terms of Wireless Services Use.

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 the 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 information systems:

- 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 information systems, 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.
- 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.
- Communicating with the media without prior approval of the Office of the Chief Communications Officer. For guidelines, refer to the USPTO Media Policy. Please refer to the DOC Policy on the Approval and Use of Social Media for explicit restrictions and guidance on the use of social media and networking sites.
- 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, your usage may be monitored at any time in order to ensure the continued operational effectiveness and integrity of the PTOnet, USPTO Wireless Network, USPTO information systems and other computing resources. Unauthorized or improper use of the information systems 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 email, 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. Official USPTO email messages forwarded to non-USPTO email addresses without authorization are not stored and maintained as federal records as required.

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.

Where an electronic record keeping system exists, the electronic message or 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 information systems provide USPTO employees to share information come with the responsibility to use the information systems 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 the OCIO-POL-19 IT Security Education Awareness Training Policy.

Appropriate use of PTOnet, USPTO Wireless Network, and USPTO information systems includes maintaining the security of the information systems, 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 PTOnet, USPTO Wireless Network, USPTO information systems and internet community), never reveal your account passwords.

Giving someone else your password is like giving them a signed blank check or a credit card. You should never reveal your password or "lend" your account to anyone temporarily. Anyone who has your password can use your account, and any activities will be traced back to your username. If your username or account is connected to abusive or otherwise inappropriate usage, the agency 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 coworkers. Never use the names of spouses, children, pets or birthdates.

The USPTO may operate a few systems which require shared accounts/passwords due to limited information system functionalities. These are exceptional cases that should be documented in the impacted information System Security Plans (SSPs) and officially approved by the organizational designated officials including the Authorizing Officials (AOs).

These password requirements are found in OCIO-POL-21, Password Management Policy.

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 wired and electronic communications. The PTOnet, USPTO Wireless Network, and all USPTO information systems are in place to facilitate the sharing of information among USPTO employees, our international partners, and 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:

- 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.
- Any email that contains Personally Identifiable Information (PII) that is sent using an automatic forwarding rule would result in a privacy breach and is a PII incident that must be reported to the U.S. Department of Commerce Chief Privacy Office and the U.S. Department of Commerce Enterprise Security Operations Center (ESOC).

Rule #5: Do not transmit classified or sensitive data, and ensure sensitive data is protected

Every attempt has been made to ensure that appropriate security mechanisms are in place for protecting information from unintended access. However, these mechanisms alone are not sufficient. PTOnet, USPTO Wireless Network, and USPTO information systems 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 email, 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.

- The USPTO Media Protection Procedures restricts access to sensitive media, including but not limited to diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks and non-digital media including but not limited to paper and microfilm, to authorized personnel within approved USPTO secure locations, based on approved access control lists.
- Do not transmit data that is part of the USPTO internal decision-making process over the internet or in public news groups.
- All USPTO management and staff are required to use their assigned USPTO email account for official communications via email.
- 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 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 email outside the USPTO network is prohibited. Auto-replies or out-of-office settings that do not use auto-forwarding are permissible. The following are examples of sensitive data that should not be discussed or transmitted on PTOnet or related computing services:
    - Any sensitive personnel data such as names with Social Security numbers, leave balances, salaries, or employee benefits.
    - Anything dealing with the details surrounding an employee relations or union issue. Union officials may store sensitive data related to employee relations or union issues as permitted by an agreement.
    - Sensitive procurement information (any procurement amounting to $1 million or more; 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.
- Do not access and use unapproved cloud storage providers from USPTO systems to transfer and store USPTO data. Use only USPTO OneDrive and Kiteworks for transferring and storing USPTO data.

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

The use of the PTOnet, USPTO Wireless Network, and USPTO information systems, including the ability to access external information via the internet, offers you an opportunity to more effectively perform your job. While using these resources, we 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:

- Copyrighted and licensed materials, including software, should not be used on USPTO information systems or collected or disseminated via PTOnet, USPTO Wireless

Network, or distributed through email or other collaboration systems without the copyright or license owner's approval.

Only software that has been evaluated, tested, and approved for use on the USPTO production network/domain may be installed on USPTO workstations in accordance with OCIO-POL-66, Workstation Software Installation and Usage Policy.

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 information systems 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 information systems 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 information systems resources, carefully evaluate your use of these resources and do not overly tax their process and store capabilities in a manner that can affect others' ability to access such resources. You are required to observe the following:

- Avoid sending email attachments larger than 20 megabytes, which is a document of approximately 60 pages of text. With embedded graphics or spreadsheets, a document could easily be 20 MB in as little as one page. Internet bandwidth usage is monitored. Please be aware of your consumption. Stick to USPTO business usage only.
- Do not stream or download games, movies and videos for entertainment purposes.
- Limit streaming or downloading of audio and video files. Media-rich communications take up significant resources and increase bandwidth consumption that can negatively

affect 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.

- 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 information systems availability by significantly impacting its performance and availability. Solutions to automated tasks need to be designed carefully by authorized staff in the Office of the Chief Information Office (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.

Rule #9: Use proper email etiquette

You are authorized and encouraged to communicate with others using the USPTO's email service whenever appropriate. Your email use enhances your ability to do work, reach message recipients, save time, and much more. Please observe the following practices:

- Keep your messages brief and to the point.
- 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?"
- When replying to an email, limit the use of "Reply All" whenever possible.
- Never share any domain account password.
- Be careful with humorous or witty messages. Colleagues who know you may understand your meaning, but strangers may interpret such messages 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. Keep in mind how you compose email to avoid appearing offensive.
- Archive email messages you need to keep after you have read them. Delete email you have read but no longer need, and delete old messages and unneeded documents from your file folders.
- Do not send email broadcast messages (i.e., messages addressed to a server and/or to all users). For messages to be widely disseminated, use authorized collaboration sites, shared folders, or an intranet page. The Office of the Chief Communications Officer can assist in coordinating agency-wide messages when appropriate.

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 remotely, and external contacts around the globe. To foster a positive experience and protect information from unintended disclosure, be aware of the following:

- Take 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 must provide proper notification when attending a meeting that is 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 during the session.
- 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. For large meetings, prepare materials in advance and have a contingency plan for any disruptions. For further details, check out virtual collaborative tools.

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

Computer viruses represent a significant threat to the operational readiness and integrity of PTOnet, USPTO Wireless Network, and USPTO information systems. Given the USPTO's increasing dependence on information processed and stored on information systems, it is important to understand and recognize the threat that computer viruses pose. 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 help prevent threats and protect our agency's assets and systems by doing the following:

- Use only U.S. government-acquired software obtained through proper USPTO distribution or requisition channels.
- Ensure any software above the image workstation baseline you received originally is approved for use on the USPTO production network/domain.
- You are prohibited from unauthorized acquisitions, use, reproduction, transmission, or distribution of any controlled information, including computer software and data that includes 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 downloading, installing or transferring any software product, including public domain freeware or shareware.

Rule #12: Protect PTOnet and USPTO information systems assets

The USPTO has heavily invested in establishing an automated environment that provides access to the computing resources and information. In order to ensure continuous service, do the following to protect USPTO assets:

- Do not reconfigure or modify USPTO computer hardware and software assets.

- Do not use IT hardware or software that has not been authorized and approved for use by OCIO, and has not been acquired through proper USPTO distribution or requisitioning channels.
- User Furnished Equipment (UFE) - You are prohibited from connecting personally owned hardware to any Government Furnished Equipment (GFE).
    - When teleworking, you may connect your service provider's router/modem to GFE (the small office/home office or SOHO router, docking station or laptop)
- Do not modify system files. Modification includes deliberate editing, changing, adding, or deleting program codes within a system file.
- Use care when eating or drinking near USPTO computers. Food crumbs and spilled drinks can cause damage to computer components.
- Do not allow unauthorized access to PTOnet resources and files. Forwarding official USPTO email and attachments to external email systems provides access to those that operate and manage those external email systems, and exposes USPTO systems to the risk of unauthorized access.
- Never attempt to cut, break or remove any lock or physical security device attached to any government-owned computer, printer, monitor, 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.
- 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's responsibility to report physical and logical IT security violations and incidents involving PII as soon as they occur (within 24 hours of the incident) by contacting the OCIO Service Desk at 571-272-9000 and servicedesk@uspto.gov or by contacting the USPTO CIO Command Center (C3) (available 24/7) at 571-272-6700 or ciocommandcenter@uspto.gov. Report all incidents and virus infections directly to the PTOCIRT (PTO Computer Incident

Response Team) by emailing CIRT, USPTO in the Microsoft Outlook Global Address List (you can also email CyberSecurityInvestigations within USPTO or from remote locations). Please refer to the USPTO Incident Response Procedures and the OCIO Incident Handling and Response page for additional details.

- Do not send an email to C3 or anyone else from the infected workstation. Please leave a voice message with sufficient detail to identify the nature of the incident and a means to contact you if C3's staff is unable to answer the phone. If you suspect that a computeris infected by a computer virus, disconnect it from the network immediately, leave it powered on, and make sure the machine is attended by someone to prevent others from using the system until a member of C3 arrives. Information systems can 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.
- Wireless devices use are not authorized for use within the USPTO (i.e., wireless mice, keyboards, etc.).
- Bluetooth devices are not permitted for personal use. OCIO-approved bluetooth devices may be used in communal conference rooms or for reasonable accommodations.
- Only OCIO-approved removable media devices may be used on USPTO computers, monitors, or docking stations. No personally owned or third-party removable media devices shall be connected to USPTO systems with the exception of OCIO Cybersecurity Divisionauthorized media transfer stations. The use of removable media devices shall be limited to the greatest extent possible and used only for pre-approved, authorized purposes in accordance to the Removable Media Policy.

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 or PIN 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 private location where your work cannot be readily seen.

- Avoid access from public wireless access points and networks since they increase the risk to individual users.

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 (UL) is authorized to connect to the Enterprise Wireless network, which requires using login ID, password, and a USPTO provided smartcard. UL is discouraged for use with USPTOGuest or PUBLIC access. 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 PTO PUBLIC via a personally-owned portable device such as a laptop computer, tablet, 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 technology our employees use when they travel to foreign countries. Please be mindful of these policies and procedures:

- All USPTO travelers must certify they have read the Defensive Travel Briefing at least annually. Travelers must adhere to all guidelines in USPTO's OCIO-POL-6 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-POL-6 Information Security Foreign Travel Policy. The form must be filled out by the

traveler and signed by a supervisor. Refer to the USPTO's OCIO-POL-6 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 overriding need for an employee to use their normal, everyday USPTO equipment overseas, OCIO staff can specially configure such equipment for business use outside of the United States. This is a significant effort, and use of pre-configured OTE is strongly encouraged. Users shall not attempt to modify configuration (including the inventory of software applications on the device) of issued USPTO approved foreign travel devices, unless the user obtains documented approval from OCIO. 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 mobile device (handhelds, tablets) 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 **only** use the USPTO-established 'alias' email account, through VPN, while overseas. The use of regular USPTO Outlook web access is explicitly prohibited.
- Employees on travel should secure equipment in locked storage when it is not directly under the your control, for instance when attending a social activity with foreign colleagues. Equipment should be in carry-on luggage when in transit.
- Do not allow unauthorized access to USPTO equipment by foreign representatives.
- 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.

Rule #16: IT Systems and related components must be approved by the Chief Information Officer (CIO). Use of Shadow IT and Hidden IT is prohibited

"Shadow IT" or "Hidden IT" refers to Information Technology (IT) systems, components, infrastructure, equipment, programs or devices that are not fully transparent to the agency CIO. This definition includes IT resources and functionality used by employees or organizations that are included as a portion of a program when it is not primarily of an "information technology" purpose, but delivers IT capabilities or contains IT resources. It also includes programs that contain a portion of its spending on equipment, systems, or services that provide IT capabilities for supporting, administering, or delivering business related functions.

- The Federal Information Technology Acquisition Reform Act (FITARA) requires the CIO to authorize the use of USPTO funds to purchase and deliver IT systems and functionality. All organizations, business units, and employees must coordinate directly with the appropriate groups within the Office of the CIO when IT systems are required in support of business requirements.
- Do not purchase or use IT systems, components, infrastructure, equipment, programs or devices in support of USPTO business that have not been authorized and approved by the USPTO CIO.
- Personal equipment, systems, or other IT components should not be used in support of USPTO business requirements.
- Enhanced privileges, IT user accounts, employee,or organization-developed software must not be used to establish alternate or customized IT functionality, develop, or install software components, circumvent security controls, or configure other IT system components (including databases, SharePoint, or other IT systems and related solutions). This prohibition is applicable and includes situations when these actions have been initiated by organizations, business units, and employees.

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 2016.

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, December 2002.
- 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.
- The Privacy Act of 1974, 5 U.S.C. §552a.
- U.S. Department of Commerce, Information Security Security Program Policy, September 2014.
- Federal Information Technology Acquisition Reform Act (FITARA).
- OMB Memorandum M-15-14, Management and Oversight of Federal Information Technology.

ISSUED BY:

Henry J. Holcombe
Chief Information Officer
United States Patent and Trademark Office

OFFICE OF PRIMARY INTEREST: Office of Organizational Policy and Governance